UNIVERSITY OF TURKU

ABSTRACT

	Bachelor´s thesis
X	Master´s thesis
	Licentiate´s thesis
	Doctor´s thesis

Subject	Operations and Supply Chain Management	Date	11.11.2018
Author(s)	Jenna Ahokas	Student number	511707
		Number of pages	69 + Appendix
Title	The Finnish Maritime Sector Inside the Cybersecurity Hurricane		
Supervisor(s)	Prof. Juuso Töyli, D.Sc. Tuomas Kiiski		

Abstract

For a long time, maritime safety and security regulations have remodeled the operations of the international maritime sector. In recent years, there has emerged a new kind of security matter called cybersecurity, which has globally remodeled even further the operations of the maritime sector. Cybersecurity and its related key factors, cyberthreat and cyberattack, have showed new kind of threats and vulnerabilities of the maritime sector. Despite the growing number of researches of related to this topic, the overall awareness of the maritime cybersecurity occurs inadequate within the international maritime sector.

The research question "How does the Finnish maritime sector experience cybersecurity?" aims at understanding the perceptions and opinions of the Finnish maritime sector's key operators, which are port authorities, port operators and shipping companies, concerning cybersecurity. This thesis was conducted as a qualitative research which was built upon a comprehensive literature review and enhanced with in-depth interviews with the key operators of the Finnish maritime sector.

The results show that the awareness within the Finnish maritime sector has increased, but there still occurs some differences between different maritime operators in terms of understanding the cybersecurity factors. The Finnish maritime operators have taken steps towards better cybersecurity, but there is still a great need for industry wide standards and practical level coordination. The NIS Directive has the chance to improve the cybersecurity operations even further and to simplify the concepts and procedures in terms of better cybersecurity situation.

Key words	Maritime sector, safety, security, cybersecurity, cyberattack
Further information	

TURUN YLIOPISTO

TIIVISTELMÄ

	Kandidaatintutkielma
X	Pro gradu -tutkielma
	Lisensiaatintutkielma
	Väitöskirja

Oppiaine	Toimitusketjujen johtaminen	Päivämäärä	11.11.2018
Tekijä(t)	Jenna Ahokas	Matrikkelinumero	511707
		Sivumäärä	69 + liitteet
Otsikko	Suomen merenkulkusektori kyberturvallisuuden aallokossa		
Ohjaaja(t)	Prof. Juuso Töyli, KTT Tuomas Kiiski		

Tiivistelmä

Merenkulun turvallisuussäännökset ovat jo hyvin pitkän aikaa muokanneet kansainvälisen merenkulkusektorin operaatioita. Viime vuosina on noussut esiin uudenlainen turvallisuustekijä nimeltä kyberturvallisuus, joka on kansainvälisesti muokannut merenkulkusektorin operaatioita ja toimintoja. Kyberturvallisuus ja siihen liittyvät avaintekijät, kuten kyberuhka ja kyberhyökkäys, ovat tuoneet esiin merenkulkusektorin uudenlaiset uhkat ja haavoittuvuudet. Huolimatta aiheeseen liittyvien tutkimuksien kasvavasta määrästä, kansainvälisen merenkulkusektorin yleinen ymmärrys ja tietoisuus merenkulun kyberturvallisuudesta on hyvinkin puutteellinen.

Tutkimuskysymys ”Kuinka Suomen merenkulkusektori kokee kyberturvallisuuden?” pyrkii ymmärtämään Suomen merenkulkusektorin keskeisten toimijoiden, jotka ovat satamanpitäjä, satamaoperaattori ja varustamo, näkemyksiä ja ajatuksia kyberturvallisuudesta. Pro gradu -tutkielma on laadullinen tutkimus, joka pohjautuu kokonaisvaltaiseen kirjallisuuskatsaukseen ja syvällisiin haastatteluihin Suomen merenkulkusektorin keskeisten toimijoiden kanssa.

Tulokset osoittavat, että Suomen merenkulkusektorin kyberturvallisuustietoisuus on kasvanut viime vuosina. Vaikka tietoisuus on kasvanut, silti haastatteluista käy ilmi suuret erot, miten eri merenkulkusektorin toimijat kokevat ja näkevät kyberturvallisuuden eri käsitteet. Suomen merenkulkutoimijat ovat ottaneet askeleita kohti entistä parempaa kyberturvallisuutta, mutta edelleen ilmenee tarve toimialakohtaisille standardeille ja käytännön tason yhteistyölle. NIS Direktiivillä tulee olemaan suuri rooli siinä, miten kyberturvallisuustoimenpiteet voivat parantua tulevaisuudessa, ja miten näitä toimenpiteitä voidaan yksinkertaistaa niin, että ne ovat entistä helpommin sovellettavissa käytännön liiketoimintoihin ja turvallisuustoimenpiteisiin.

Asiasanat	Kauppamerenkulku, turvallisuus, kyberturvallisuus, kyberhyökkäys
Muita tietoja	

UNIVERSITY OF TURKU
Turku School of Economics

THE FINNISH MARITIME SECTOR INSIDE THE CYBERSECURITY HURRICANE

Master´s Thesis
in Operations and Supply Chain Management

Author:
Jenna Ahokas 511707

Supervisors:
Prof. Juuso Töyli
D.Sc. Tuomas Kiiski

11.11.2018
Turku

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin OriginalityCheck service.

Table of contents

List of figures

List of tables

List of appendices

List of abbreviations

AIS	Automatic Identification System
APT	Advanced Persistent Threat
BIMCO	Baltic and International Maritime Council
CEO	Chief Executive Officer
CPS	Cyber-Physical System
DoS	Denial of Service
DDoS	Distributed Denial of Service
ECDIS	Electronic Chart Display Information System
EMSA	European Maritime Safety Agency
ENISA	European Union Agency for Network and Information Security
ERP	Enterprise Resource Planning
EU	European Union
GDP	Gross Domestic Product
GMDSS	Global Maritime Distress and Safety System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
ICAO	International Civil Aviation Organization
ICS	Industrial Control System
ICT	Information and Communication Technology
IMO	International Maritime Organization
ISM	International Safety Management Code
ISPS	International Ship and Port Security Code
ITS	Intelligent Transport System
MGCI	Maritime Global Critical Infrastructure
MSC	Maritime Safety Committee
MSW	Maritime Single Window
MTS	Maritime Transport System
NESA	National Emergency Safety Agency
NSW	National Single Window
PCS	Port Community System
SOLAS	International Convention Safety of Life at Sea
SSN	SafeSeaNet
UHF	Ultra-High Frequency
UNCTAD	United Nations Conference on Trade and Development
VHF	Very-High Frequency
VTS	Vessel Traffic Service
Wi-Fi	Wireless-Fidelity

1 INTRODUCTION

1.1 Background

Recently, the interest in cybersecurity, which usually refers to the protection of both physical and technological assets of companies, has increased globally due to several factors. First, digitalisation in the world is continuously growing, which has led to great dependence on efficient information systems. Second, these information systems, and the information and data stored in them are located in a digital environment called cyberspace of which characteristics are complex. (Goldby 2008; Fitzgerald et al. 2013.) Third, the reliance on technology and different information systems has made societies and companies vulnerable to the functionality of these information systems (Carrapico & Barrinha 2017). Fourth, the number of cyberattacks has shown a year-by-year increase and has caused considerable financial losses to societies and businesses (Colesniuc 2013). Even, some researchers have noticed the upcoming of the Fourth Industrial Revolution, which has the potential to even increase the degree to which organisations and industries rely on various Information and Communication Technologies (ICT) and systems (Johanson 2016; Teoh & Mahmood 2017).

The emergence of new ICT systems has brought a fundamental shift in the way nations and their citizens are involved in global economic activities, such as, how they control critical infrastructure, and communicate with each other (Stahl 2011). It has been identified that malicious acts performed by individuals and groups through cyberspace towards the important systems have been listed alongside natural disasters and terrorism (Kapto 2013). Also, the motives behind cyberattacks differ greatly from one another, consisting of excitement, money and political agendas (Ahokas & Kiiski 2017a). Nowadays, it has been recognized that cyberrisks not only include identity thefts and cybercrime, but also threaten national and international security (Stevens 2013).

The biggest cyberattacks in 2017, WannaCry and NotPetya, revealed internationally the vulnerabilities of critical infrastructure, which includes facilities, networks, and assets impacting on economic and social functionality of a certain nation (Borum et al. 2015). Since the maritime sector has a significant role in the global transport networks, it can be seen as a backbone of global trade and a part of the critical transport infrastructure (Di-Renzo et al. 2015). Globally, approximately 80 per cent of the world trade is transported by sea (UNCTAD 2017; Jensen 2017).

New information technologies and systems play an essential role in all transport modes. They have a great impact on the efficiency, consistency, and performance of global transport networks. (ENISA 2011; Fok 2013.) Especially, the maritime sector has faced the fact that cybersecurity needs to be included in physical security systems and

strategies. Both domestic and international port facilities depend as much on networked computers and information systems as they do on the manpower to confirm the flow of maritime commerce on which the economy, the homeland, and the national security rely. (Shah 2004; Škrlec et al. 2014.)

The maritime sector has not been able stay immune to the radical changes of new digital technologies and systems which may be disruptive (Fitton et al. 2014; Frøystad et al. 2017). Therefore, cyberattacks towards the maritime sector have increased (Burton 2016), and especially the NotPetya cyberattack was capable of disrupting the operations of Maersk's 17 APM Terminals across the world (Kiiski 2018). It made the international maritime industry realize its vulnerability towards cyberattacks. It also highlighted that there are no specific guidelines or responses in place to mitigate or prevent a major cyberattack. (Jensen 2017.)

The first report, which highlighted the lack of awareness of cybersecurity in the maritime sector, was published by the European Network and Information Security Agency (ENISA) in 2011 (ENISA 2011). Since then, the academic interest towards cybersecurity as well as maritime security has remained low (Hult & Sivanesan 2013; Germond 2015). Although some international and national strategies for cybersecurity have been published, the academic interest towards maritime cybersecurity seems far more uncharted subject, even though some other theses have been written around this subject (Ahokas & Kiiski 2017a). In 2017, Ahokas and Laakso (2017) established fresh empirical findings from the Baltic Sea Region highlighting the inadequacy of cyberthreat preparedness and regulation in ports.

1.2 Research objectives and structure of the study

The main focus of this study is to analyze the criticality of cybersecurity and its various issues in the maritime sector. From literature perspective, the current situation and awareness in the global maritime industry seems quite inadequate and needs more researching in terms of responsibilities and liabilities. The study tries to understand the effects of cybersecurity factors in the maritime sector, in particular the Finnish maritime sector, and how the different maritime operators and authorities see the responsibilities and obligations concerning cybersecurity and cyberattacks. The overall target is to get a a comprehensive idea and picture of the cybersecurity and the issues related to the subject rather than specifically point out the vulnerabilities and ICT systems of the maritime sector and guide on how to protect them. The aim of the study is approached with the following question:

1. How does the Finnish maritime sector experience cybersecurity?

Different motives were found to drive this study further. There is a limited amount of publications and empirical data available, because of the novelty and diverse nature of the topic. For example, Bou-Harb et al. (2017) have also indicated the lack of real malicious empirical data that could be captured, inferred and analysed within the operational boundaries of such as Cyber Physical System (CPS). Also, the terminology behind cybersecurity is far from being consistent as the use of various concepts with different meanings is common. For example, the relationship between cyberthreats and cyberattacks has been difficult to identify (see Kadivar 2014; Loukas 2015). In order to provide input to this issue, a conceptual map was presented by Ahokas et al. (2017b) that delineates the relationships between different concepts.

The study has been divided into background Chapters and research Chapters. Chapter 2 identifies the difference between maritime safety and security and presents the characteristics of the global and Finnish maritime sector. It also indicates the key information systems that are needed more or less for the maritime operations to be efficient. Chapter 3 illustrates and clarifies the key concepts related to cybersecurity. The conceptual map by Ahokas et al. (2017b) and its key concepts are explained in Chapter 3. Through the conceptual presentations of the key cybersecurity related concepts is presented the current state of maritime cybersecurity based on the published researches and articles. Chapter 4 indicates the specific research methods and research phases of this study. In the fifth Chapter, the main findings of this study and its survey are brought together. Chapter 6 summarizes the study and its main findings related to the case/survey and also addresses some proposals for future researches.

The research is compiled from the perspective of an outsider researcher rather than from the perspective of the maritime sector or a single port. As for this study, the maritime sector includes ports with their port authorities and operators, and the shipping companies related to cargo operations as these actors are in direct connection to global maritime trade. The ship building industry has not been taken into consideration in this study as they are not directly related to the movement of cargo based on daily maritime operations.

2 CHARACTERISTICS OF THE MARITIME SECTOR

2.1 Identification of maritime risk, vulnerability, and threat

In order to comprehensively understand how the key maritime safety and security regulations have remodeled the industry as a whole, it is crucial to go through the concepts of maritime risk, vulnerability, and threat. Risk and threat alongside with security are necessary concepts when examining any business environment. A risk can be seen as a probability of an event which has the opportunity for either positive or negative consequences (Prezelj & Ziberna 2013). The main difference between risk and security is that the last-mentioned involves also uncertainty (Marlow 2010).

Risk can be understood as the potentiality of harm, which will be attained under the conditions of use and/or exposure, and the possible extent of the harm (Fransas et al. 2012). The maritime sector is vulnerable especially in terms of operational risks, such as accidents, failures in equipment or mishandling of dangerous cargo, labour strikes, and security breaches, which include direct physical attacks, sabotage, and thefts (Kouwenhoven et al. 2016). In ISPS Code, IMO (2012) has identified that a risk contains aspects, such as, threat, impact, and vulnerability. Polemi (2018) has expanded the definition of risk by adding other dimensions, such as, likelihood of threat, average loss of threat, and likelihood of incident.

The following five risk categories: 1) Technical, 2) Financial, 3) Political, 4) Market, and 5) Environmental have been identified to occur within the maritime sector. Technical risks are often internal and occur from constructions and technology. Financial risks include, for example, fluctuations of interest rate, taxation currency, and organization's own capital risks, such as, loan availability. Political risks include legal, regulatory and moral hazards. Market risks occur from economical changes in market areas, and include various factors influencing business models and environments. Environmental risks relate to changes of environmental laws and unforeseen societal sensitivities. (Rodrigue et al. 2011.)

Vulnerability factor	Methods of implementation of vulnerability factor
Cargo	Smuggling of people, drugs or other illegal weapons
External impacts	Damage to property Disturbance of trade flows Loss of life
Vessels	Disruption of infrastructure by sinking vessels Possibility to use as a weapon to launch an attack
People	Attacking vessels to provoke human casualties
Money	Revenues from shipping can be used to fund terrorist activities

Figure 1 Vulnerabilities of the maritime sector (McNicholas 2008; Kouwenhoven et al. 2016)

In Figure 1 is presented the most common **vulnerability** factors of the maritime sector. Other examples of the vulnerabilities include situations in which a ship is attacked by terrorists in a manner of political act or cargo is hijacked by pirates or criminal groups. Behind these cargo hijackings, the motives vary from being a political act to generation of funds. Containers are often used as a transport method in different transnational crimes, such as smuggling of drugs, weapons or humans. (Forbes 2003; Kouwenhoven et al. 2016.) Cargo theft can be seen as the biggest problem for the whole maritime sector. It has been estimated that globally cargo thefts costs approximately $30 billion per year. (Edgerton 2013.)

The International Civil Aviation Organization (ICAO, 2008) identifies ***hazard*** as "a condition or an object with the potential of causing injuries to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function". Therefore, wind and other weather conditions can be seen as examples of the maritime hazards (Fransas et al. 2012).

Threat can be understood as an act or actor that can bring harm or damage to a country, organisation, person or facility (Polemi 2018). In the maritime context, threats consist of all the possible harmful or damaging activities that are carried out by nation-states and their proxies or terrorists, and criminal groups or individuals not acting on behalf of a nation. (Edgerton 2013.) Maritime threats include, for example, physical disasters, sabotage, terrorist attacks, financial losses and theft of cargo or information (McNicholas 2008; Loh & Thai 2015).

2.2 Maritime safety

In order to understand the link between the motivation of this study and the literature background, highlighting the difference between safety and security in contrast to the maritime sector is necessary. Any clear or common theory for safety and security cannot be found in existing literature. The connection between safety and security can be seen in various ways. Many authors and researchers have indicated that safety forms a bigger and more comprehensive concept, and security can be placed within the safety measures, and this relationship is indicated in Figure 2. (Helmick 2008; Polemi 2018.)

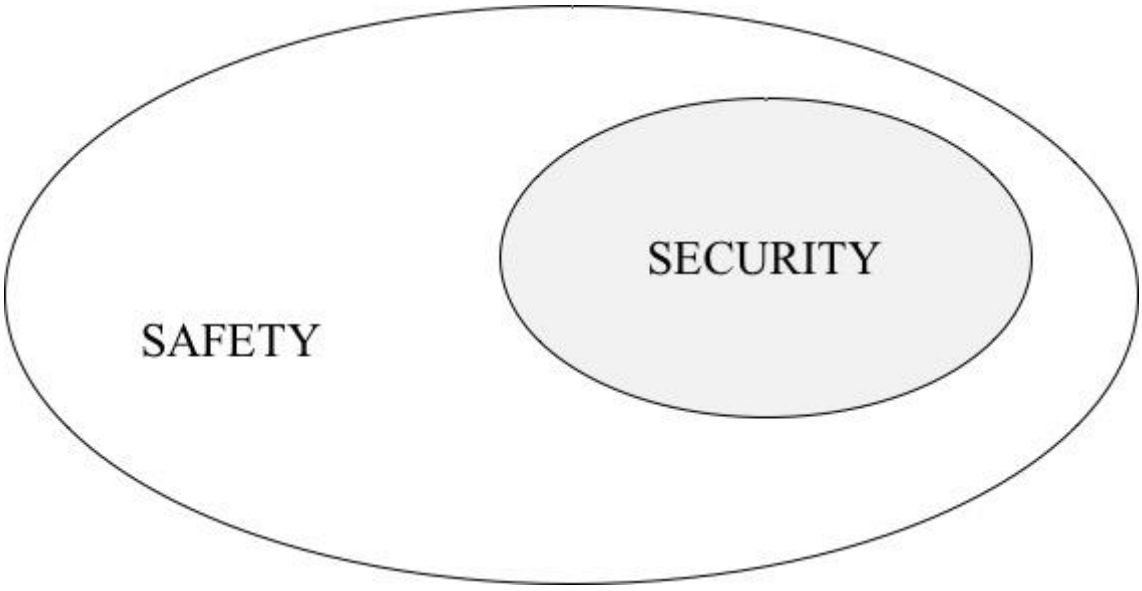

Figure 2 The relationship between safety and security (Polemi 2018)

Maritime safety can be seen as the set of preventive measures projected to protect the global maritime sector against, and to reduce the effect of unintentional or natural danger, harm, risk or loss (Edgerton 2013). Maritime safety can also be identified as the safety of life and protection of assets at sea from the environmental and operational threats, and also the safety of maritime environment from pollution by the ships. Most of the time, maritime safety includes all the aspects related to the combination of safety and security. (Fransas et al. 2012.)

The following four factors 1) external safety; 2) internal safety; 3) human factor; and 4) environmental impacts are used to describe maritime safety. External safety includes, for example, fairways, ports, related equipment and environmental conditions. Internal safety influences the structure and damage stability of ships, and assessment of commercial premises. Human factor is an important factor related to maritime safety, because almost 80 % of incidents and accidents are caused by the human factor. Environmental

impacts are caused by the complicated interactions between all of the previously mentioned factors. (Fransas et al. 2012, 12.)

The maritime safety sector with all of its operational institutes is ruled by a strong global regime. But it can be seen that all the national maritime safety regulations and guidelines follow the main points and structures of the International Maritime Organization's (IMO) maritime safety Conventions and Codes. The Code and regulations of IMO are easier to acknowledge and implement in the operations of the maritime operators. (Guldbrandsen 2013.) Due to major accidents within the maritime sector, two main maritime safety regulations have been developed: International Convention for the Safety of Life at Sea (SOLAS) and the International Safety Management (ISM) Code (Attard 2014).

SOLAS Convention has long been identified to be the primary consideration in comprehension of safety at sea as it is one of the oldest Conventions of IMO. The first edition of SOLAS was adopted in 1914 after the tragic sinking of Titanic in which 1,500 lives were lost. At the beginning, SOLAS aimed to set international shipping practices and regulations for seafaring vessels. After that, four different version have been published and adopted since 1914. (IMO 2014a; Hayes 2016.) After the terrorist attacks of 9/11, SOLAS was reformatted to include also the prevention and mitigation of terrorist acts against ships and also to enhance maritime security aboard ships and ashore. The current objective of SOLAS Convention is to provide minimum safety standards for construction, equipment, and operation of ships. (Attard 2014; Polemi 2018.)

The instructions of SOLAS include also international standards for areas, such as life-saving requirements, navigational safety, crew licensing and competence, and vessel management (Edgerton 2013). The instructions of SOLAS are directed for the shipping industry, but there are some references to ports and to ship-to-port interfaces that include all the interactions when a ship is directly affected by actions including the movement of humans, goods, or the provisions of port services to and from ships. In SOLAS has been identified that maritime safety information refers to navigational and meteorological warnings, meteorological forecasts and other required safety related messages broadcast to ships. (IMO 2014a.)

ISM Code is another main Code increasing the safety of the maritime sector by instructing the maritime operators to take responsibilities of the safety and security issues of their operations (Fransas et al. 2012). The code was adopted in 1993, and five years late in 1998 it became mandatory for passenger vessels, passenger high-speed crafts, oil and chemical tankers, bulk carriers, and cargo high-speed crafts of 500 gross tonnage or more. After 2002, mandatory nature of ISM was expanded to include other cargo ships and self-propelled mobile offshore drilling units of 500 gross tonnage or more. (McNicholas 2008; IMO 2014b.)

The key objective of ISM is to advance safety culture within the maritime sector and continuously enhance this issue, and it has affected the safety levels of the maritime sector (Lappalainen et al. 2010). In 2010, IMO published the new amendments for the code that included the factory of risk assessment, which requests the company to impose all known and identified risks to ships, personnel and the environment of the company, and to develop appropriate safeguards. ISM covers the maritime safety in more general level, it does not go into details in terms of specific maritime operators. Therefore, this Code is not suitable for ports to use it as a guidance for their safety measures. Thus, ports are more likely to follow the International Ship and Port Facility Security (ISPS) Code and its security measures. (Salokorpi & Rytkönen 2010.)

2.3 Maritime security

Security as a concept refers to the assurance of confidence, integrity, reliability, and availability, but it has various multidimensional meanings (Brooks 2010; Polemi 2018). Often security is used to pointing out the intentional threats in contrast to ones with unintentional or natural origin (Edgerton 2013; Craigen et al. 2014). Maritime security has been a significant issue for ports, shipping companies, insurance companies, and relevant international and national organisations and institutions (Bou-Harb et al. 2017). As a term, maritime security was almost absent from the debates until the beginning of the 2000's. Thus, the following three factors have increased the buzz around the term: 1) the impacts and consequences of the 9/11 terrorist attacks, 2) the occurrence of three high visibility terrorist acts against ships, such as USS Cole in 2001, French tanker Limburg in 2002, and Filipino passenger ship SuperFerry14 in 2004, and 3) the rise of piratical attacks in the Strait of Malacca at the beginning of the 2000's. (Germond 2015.)

Maritime security can be identified as a set of preventive actions to defend the maritime sector against hazard and intentional illicit acts, but it also includes the secure feeling of the shipping company, vessel, crew or port against threats, such as piracy, terrorism, and other criminal activities (Helmick 2008; Germond 2015). The intentional and illicit acts refer to planned and appropriate actions that aim to cause harmful damage to their targets. Sabotage, espionage, vandalism, terrorism, piracy and theft are seen as intentional actions. These security risks and threats include organized criminal activities, such as extortion, smuggling and human trafficking. (Andritsos & Mosconi 2010; Fransas et al. 2012; Bueger 2015.)

As the dependence on ICT systems grows, the aspects of physical security need to be updated to a sufficient level in terms of the security of ICT and physical-related components of the maritime sector (Fitton et al. 2014). The ISPS Code aims at ensuring that all sensitive information is protected with a password, access-control and security systems

are installed in locations where sensitive information is stored, and effect data back-up procedures have been installed. Even though cyberattacks have increased, there has been no moves in terms of implementing or modifying the essential Convention and Codes to tackle and mitigate cyberattacks through cybersecurity frameworks. (IMO 2012; Polemi 2018.)

ISPS Code was established after the 9/11 terrorist attacks, and due to these attacks, the international maritime community re-evaluated the existing safety laws and found it reasonable to reform SOLAS Convention (McNicholas 2008). ISPS Code was adopted and published in December 2002, but it only entered into force worldwide on 1 July 2004 (Helmick 2008). The Code highlights port security against the threats related to maritime security, and it identifies and provides precautionary measures concerning security related conflicts (Shah 2004). Nowadays, ISPS is a notable development in the laws relating to maritime security. ISPS Code is internationally the most relevant legislation on port security. Code is mandatory for passenger and cargo ships of a minimum 500 gross tonnage with international voyages, mobile offshore drilling units and port facilities. (Shah 2004; Attard 2014.) ISPS Code has also been implemented at the European Union (EU) level by the EU/725/2004 and the EU/65/2005, which mandate the recognition of authority, acts skills and objectives to set up and sustain security measures (Chiappetta & Cuozzo 2017).

ISPS Code is divided into two different parts. Part A emphasizes the principles that maritime stakeholders should comply with, and it is the mandatory part of ISPS Code for ships and port facilities. Part B highlights different ways on how the principles can be put into operation, and it provides guidelines for the processes and procedures, which are needed in implementation of the requirements and standards issued in Part A. (McNicholas 2008; Attard 2014.) In this Code IMO has highlighted the five specific security issues: 1) Piracy and armed robbery, 2) Drug smuggling, 3) Stowaways, 4) Illicit migration, and 5) Security of dangerous cargo. (IMO 2012.)

The key objective of ISPS Code is to efficiently evaluate and analyze threat and risk possibilities in three different security levels. These security levels refer to the degree of risk that a security incident is likely to happen or be attempted. The security incident includes any suspicious act or circumstance threatening security of a ship or a port, including mobile offshore drilling units and high-speed crafts, or any ship-to-port interface or any ship-to-ship activities. The three main security levels control the security requirements of the ships and ports. If a port has announced its status to be the security level 2, a ship with a security level 1 cannot enter this port without raising its own security level to meet up with the port's security level. (IMO 2012.)

2.4 Maritime sector in general

In order for a modern society to function efficiently in all of its functions from the supply of raw materials to every product on the shelves of the local stores and supermarkets, it needs to have effectively working maritime sector (Shah 2004; Chiappetta & Cuozzo 2017). Around 80–90% of the goods carried through international trade in the world depends on the maritime sector and maritime transport (UNCTAD 2017). The maritime sector consists of globally distributed organisations, such as port authorities, ministries, maritime and shipping companies, customs agencies, maritime and insurance companies, other transport critical infrastructures, for example, airports, transport networks, energy networks and telecommunication networks, and many more (Polemi & Papastergiou 2015). Ports as a part of global maritime supply chains form the backbone of global trade and economy (Chiappetta 2017; Polemi 2018).

The maritime sector is a part of a global and continuously changing network (Kallionpää et al. 2013). There are two terms used to identify the different actors and operations of the maritime sector. It can be identified with the term Maritime Global Critical Infrastructure (MGCI), which includes all of the infrastructures, such as, ports and straits that have the ability to inflict over boundary and multi-sector impacts on the society of a nation in terms of disturbance. MGCI includes all the systems and assets that rely on specific maritime activities and are capable to internationally impact security, global economic security, public health and safety. (Kajitani et al. 2013.) The Maritime Transport System (MTS) highlights the criticality of the maritime sector to global economy. MTS includes ports, waterways, and their intermodal operators, such as, port authorities, port operators and customs. (Helmick 2008; DiRenzo et al. 2015; Polemi 2018.)

The operations of the maritime sector can be roughly divided into land operations and shipping operations. The shipping industry with its shipping companies offer the shipping operations, which are the key element in maritime transport. The key actors of the land operations of the maritime sector are port authorities, who maintain the port infrastructures, and port operators, who handle the cargo operations related to loading and discharging of vessels. (Jensen 2017; Polemi 2018.)

Ports form the center point of operations related to shipping and other maritime operations. Ports comprise critical intermodal nodes in cargo and passenger transport networks and significant border control points, which highlights the importance of installed and effective security policies (Andritsos & Mosconi 2010; Demirbas et al. 2014). Due to the connectivity of ports between countries, they are seen as strategical interfaces within the maritime sector. It is difficult to identify ports comprehensively due to their various activities, which are dependent on the size of the port and the offered services. (Trujillo & Tovar 2007.)

Traditionally, a port contains a port authority, port superstructure, such as cranes and conveyors, and infrastructure, loading and unloading functions, storage facilities, and intra-port operations (Brooks & Cullinane 2007). Port authority plays an essential role in the international trade and within the maritime sector (Chiappetta 2017) and has the responsibility to maintain and take care of the main land areas and basic infrastructures. (Ojala 1990; Helmick 2008.) The role of port authority in governing the regionalization phase can differ a little according to the type of port exploitation. When the state of a municipal government represents the port authority, it is responsible for the land access infrastructure. In this case, the port authority is seen as a landlord, who provides the infrastructure to various operators, for example, carriers, shippers, and transport operators. (Notteboom & Rodrigue 2005; Yliskylä-Peuralahti et al. 2011.)

The nature of port operations has been identified as heterogeneous, and operations are nowadays provided by different operators, such as shipping lines, terminal operators and stevedoring companies (Helmick 2008; Meersman & Van de Voorde 2010). Usually, port operators lease the facilities and only invest on their own staff and personnel. As the most essential role of the operators is to provide and coordinate the cargo loading and unloading plan for the terminal or vessel and move the unloaded cargo to a warehouse or to its consignee. Operator will also have a relationship with the ministries and customs of a port in terms of providing, for example, required clearance documents. (McNicholas 2008.) These port operations, such as cargo handling, warehousing and custom services, rely on various of ICT systems of different actors of the maritime sector (Polemi 2018).

Ports also include the port facilities, which can be understood as areas of land or water, or land and water. These land areas are used either wholly or partly for an embarkation or disembarkation of passengers, or with loading and unloading of cargo from ships. The ship-to-port interface occur within the port facilities. In port facilities are included areas of anchorages, waiting berths, and approaches from seaward. (Andritsos & Mosconi 2010; IMO 2012; IMO 2014a.) The port facilities can be divided into port infrastructure and superstructure. Port infrastructure refers to berths, docks, basins, warehousing areas and internal connections inside the port area. Port superstructure consists of required equipment for the loading and unloading processes of cargo, for example, cranes and conveyors, stackers and forklifts, and also container stacking and storage of goods. The difference between superstructure and infrastructure is that former is often privately owned. (Paixão & Marlow 2003; Yliskylä-Peuralahti et al. 2011.)

Maritime companies include, for example, stevedoring companies, which can be seen as a company, which a port operator can hire to provide the machinery, hire the laborers to work the vessel, and control the execution of the loading of cargo, which will leave the terminal (McNicholas 2008). Together with ports, the shipping industry is seen as the blood vessels of international trade and as the facilitator of the global economy's expansion (Christiansen et al. 2013). IMO (2014a) has identified the different ships of the

shipping industry. Just to mention a few amongst the many different ships: a passenger ship is considered to be a ship which carriers more than twelve passengers, a cargo ship is roughly identified to be any ship, which is not a passenger ship and a tanker is one of the many forms of cargo ship, which is structured to carry in bulk of liquid cargoes of an inflammable nature.

In order for all the maritime operators to provide their services efficiently, they need their business environment to be secured. The maritime business environment can be divided into two environments: 1) physical environment, and 2) cybernetic environment that are presented in Figure 3. The physical environment contains various actors, such as authorities, maritime and insurance companies, and human resources, and facilities, such as, the port infrastructure, for example, different buildings, gates and platforms within a port. On the other hand, the cybernetic environment includes also the port infrastructure, and ports' ICT systems, such as networks, ICT hardware equipment, Port Community Systems (PCSs), services, data, and users, and telecommunications systems. (Dellios & Papanikas 2014; Polemi 2018.)

PHYSICAL ENVIRONMENT	CYBERNETIC ENVIRONMENT
Port infrastructure, facilities, gates, platforms, marinas and data centres	Infrastructure, such as buildings and ships
Port authorities	Platforms, such as servers and databases
Maritime and insurance companies	Telecommunication systems, such as networking terminals and geographic information systems
Shipping and cargo industry	Software and manuals, such and information and data
Manufacturers and suppliers	E-services, such as applications, frameworks, and test environments
Government ministries	Other equipment, such as fire alarm and extinguisher systems, and surveillance systems
Related transport infrastructure	Internal users, such as administrators and personnel
Human resources	External users, such as port authorities and maritime companies

Figure 3 Physical and cybernetic environment of the maritime sector (Dellios & Papanikas 2014; Polemi 2018)

As indicated in Figure 3, the operations of ports rely on the physical environment and infrastructures within port areas, but they also require a stable base of ICT systems and infrastructures (Papastergiou et al. 2015). Even though, the environment structure is basically the same for each operator of the maritime sector, the role of ports within the maritime sector creates a central difference between these two factors. Ports form a sole

entity, which interacts directly with all the other maritime entities and provide services with different degree of criticality. Due to the large-scale infrastructure of ports and the degradation, disruption, or impairment of ports' physical or cyber systems, ports are seen as a part of the transport critical infrastructure that may have critical consequences on national health, security and safety, economy, and welfare of citizens. Because of these physical and cyber systems include large amount of critical and sensitive data, information and services, and various interdependencies with other critical infrastructures, they are seen to be vulnerable, for example, to hazardous accidents and cyberattacks. (Polemi & Papastergiou 2015; Polemi 2018.)

2.5 Key information systems of the maritime sector

Throughout the years, the maritime sector has been dependent on different communication methods, and it has been an area of which interest increases all the time (DiRenzo et al. 2015). The traditional information flows have relied on paper, and therefore have increased operating costs and decreased the satisfaction of customers. Electronic information has reduced logistics expenses and increased the satisfaction of customers by increased coordination. (Muthiah 2009; Polemi & Papastergiou 2015.) Due to the increased dependence on new information technologies and systems, the maritime sector is seen as one of the key sectors for digital transformation (Fruth & Teuteberg 2017).

The new technologies have often pressured maritime operators to intensify their infrastructure in order to maintain their operations and to respond to market requirements (Bou-Harb et al. 2017; Polemi 2018). This dependence on and development of new ICT systems has enabled the maritime sector to increase its productivity and to meet the operational requirements (Beaumont & Wolthusen 2017). Still, the main applications used in shipping industry are text messaging, email, video, web surfing, collaborative planning voice, and Automatic Identification System (AIS) (Manoufali et al. 2013).

Current ICT systems are used to enhance the necessary maritime operations, for example, navigation, freight management and traffic control communication (ENISA 2011; Polemi & Papastergiou 2015). Ports use information technology systems to track maritime cargo, trucks, and trains, but they also use it to optimize the cargo loading and unloading processes (Heilig & Voß 2016; Bou-Harb et al. 2017). The effective ICT systems assists ports to manage, store, and exchange information data and to provide electronic and/or mobile port services to different maritime operators (Tijan et al. 2014; Polemi 2018). The essential ICT systems of ports form a part of the core of intelligent transport system (ITS) (Fok 2013).

Ports are involved in multiple information flows depending on different ICT systems. This means that every data that is exchanged and saved in ICT systems is a potential

threat in form of a possible entry point for unauthorized access to the ICT systems. (Kouwenhoven et al. 2016; Bosse & Stamer 2017.) The dependence on ICT systems is as great as the dependence on stevedores lifting and hauling goods, and the systems of tracking cargo are not the only systems within a port that can be considered as a target of cyberattack (DiRenzo et al. 2015). The vulnerability of traditional ICT systems and Industrial Control Systems (ICS), which include supervisory and distributed control systems, can be seen as one of the main reasons why ports have started to develop CPSs. This emergence of CPS has created a major gap of recognize comprehensively the features of malicious attackers and their capabilities, intentions, and aims, when they are targeting a certain system. (Bou-Harb et al. 2017.)

In Figure 4 presents the connection between different maritime operations and essential ICT systems. These ICT systems need other technologies to support and enable the connection and communication between different operators. For example, the Vessel Traffic Services (VTS) needs to have data from Global Positioning System (GPS), Electronic Chart Display and Information System (ECDIS) and Automatic Identification System (AIS) to have a comprehensive picture of the situation at sea. (Heilig & Voß 2016.)

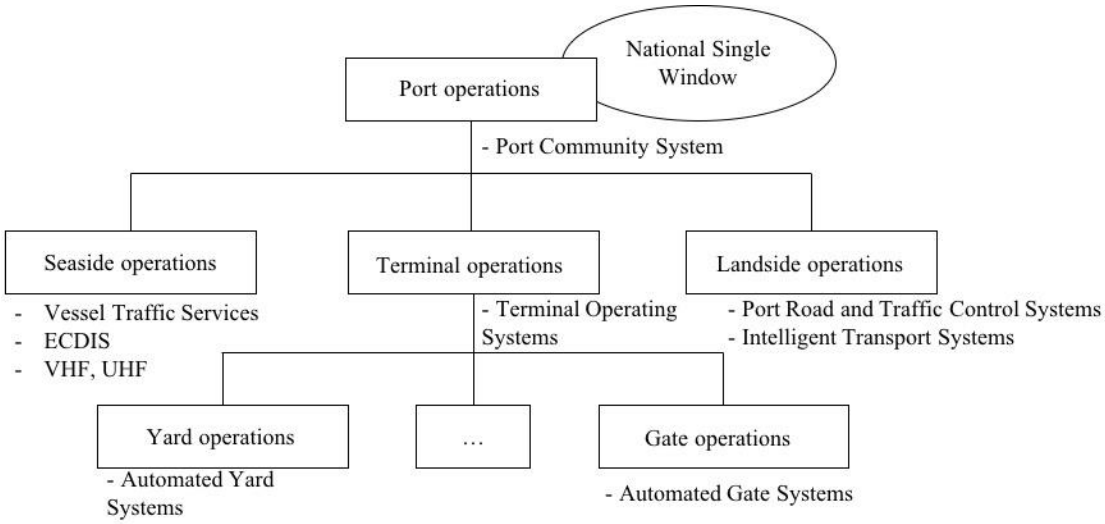

Figure 4 Identification of port-related information systems (Heilig & Voß 2016)

In Figure 4 the legacy ultra-high frequency (UHF) or very-high frequency (VHF) are located under seaside operations, because they are mainly used between ships and ports or ships and ships. Both of these have a small capacity and cannot support high data rate applications. They are used, for example, when a ship is coming to a port and needs to inform its position and route inside the port to port authorities. (Manoufali et al. 2013.) VHF radio is mostly used in ship-to-ship and ship-to-shore voice communications because its range is about 20 nautical miles (Du et al. 2010). The proper use of VHF radio has been highlighted in IMO's Global Maritime Distress and Safety System (GMDSS)

manual, which entry into force in February 1999. GMDSS manual highlights that every ship, while at sea, needs to maintain, where practicable, a continuous watch on VHF channel 16. Therefore, in each ship in the world needs carry a VHF equipment. (IMO 2017.)

There are three main ICT systems, which are essential for ships in the maritime sector: AIS, GPS, and ECDIS. The main similarity between these systems is that they are not in a direct connection with the Internet. There are also three other ICT systems, PCSs, National Single Window (NSW) and Maritime Single Window (MSW) that have influenced the maritime communication and transport in recent years. (Muccin 2015.)

The first version of ***Automatic identification System (AIS)*** was developed in the late 1980's and early 1990's when it stood for a transponder for ships to help in the identification of vessels in VTS. Since 2004, AIS been mandatory in ships, such as passenger ships and sea-going vessels with the capacity of 300 gross tonnage, by IMO's ISPS Code to increase maritime safety and security. It is a telematics system within the maritime sector, which performs automatic data exchange among ships. It has significantly improved the safety of navigation, especially in conditions, where visibility is limited. (Manoufali et al. 2013; Balduzzi et al. 2014.) Therefore, it is the most vital technological advances in terms of maritime safety (Page 2017). As indicated in the Regulation 19 of SOLAS Chapter V, AIS broadcasts various data about ships, such as location, name, length of the ship, destination port, and expected time of arrival, automatically and periodically. With AIS information can be avoided, for example, collisions of ships, and also its helps to communicate with shore-based VTS. (Manoufali et al. 2013; Balduzzi et al. 2014.) AIS provides also data about maritime traffic and can receive information sent from terrestrial AIS transmitting stations via VHF (Fruth & Teuteberg 2017; Page 2017).

Even though, AIS uses a VHF radio to communicate with VTS and other ships, it is not a GMDSS communication system (IMO 2017). AIS does not include any built-in security measures or verification system, which could provide a level of backup, and the information is automatically assumed to be genuine. Therefore, it is extremely vulnerable to external threats. When targeting AIS in a harmful way, an attacker could, for example, falsify the identity, type, position, heading, or speed of a vessel. (Balduzzi et al. 2014; DiRenzo et al. 2015.)

In the middle of 1990s, was invented the Global Navigation Satellite System (GNSS), which led into the effective installation of ***Global Positioning System (GPS)***. GPS has been implemented around the globe working daily and the performance depends on the satellites. GPS was developed in the United States in 1960's as a part of NAVSTAR process. As a product, GPS was founded in 1973, but the building of GPS was started in 1978 and the finished product was put into market in 1995. GPS has been formed to be reliable and accurate positioning system. In logistic operations, GPS has been used to detect and track movable objects, such as containers, vessels, equipment, and vehicles. It

is also used to aid navigation and route planning, and in tracking deliveries real-time. Still, it has not reached its full potential in logistic operations. (DiRenzo et al. 2015.)

Ports use GPS for real-time data on the position and status of objects which has improved both visibility and effective planning and coordination of activities, which traditionally have involved multiple actors (DiRenzo et al. 2015; Heilig & Voß 2016). For ships, GPS has improved the arrival times to be more accurate, enhanced smarter container technology, and is capable to deliver real-time weather data (Fruth & Teuteberg 2017). GPS systems in particular are seen as vulnerable to unintentional interference and jamming, which may result in possible Denial of Service (DoS) attack over large geographical areas (Burton 2016).

On March 24, 1988 a tanker ship Exxon Valdez hits the Bligh Reef only after leaving the channel in Prince William, and spills 42 000 m^2 of oil. The environmental and damage costs rose up to USD 3 billion. After this accident, IMO and Hydrographic Organisation finished their ***Electronic Chart Display Information System (ECDIS)*** standards, which allowed mariners to navigate along coastal waterways. It is an electronic chart navigation information, which integrates data from the GPS, speed log of a ship, gyrocompass, and radar, and uses electronic charts, which are supplied by a national hydrographic office. (Dooling 1994; Muccin 2015.) The ECDIS standard was approved by the Maritime Safety Committee (MSC) in May 1994 and adopted as an Assembly Resolution in November 1995 (Grant & Goodyear 1996). Under the regulations of SOLAS Chapter V, ECDIS has been made mandatory for most large vessels, and the deadline for entry into force comes to end on July 1, 2018 (Whyte 2018).

ECDIS provides visualization of all paper chart information on a computer screen and also a broad range of other data, which is essential for navigational purposes. It is a computer-based information system, which delivers real-time display of the navigator's own vessel located with reference to the surrounding sea area. (Becker-Heins 2014.) It has increased the overall safety of navigation within the maritime sector. ECDIS also provides automatic route monitoring, which include warnings and indications of hazards to the operator and in time arrivals. (Grant & Goodyear 1996; Becker-Heins 2014.) Larger ships are required to have two ECDIS's on the bridge of the vessel as the other one is there for backup. The problems of ECDIS occur from system updates, as the updates are downloaded from external source though a USB port via a memory stick or via the net. (Muccin 2015.)

A ***Port Community System (PCS)*** aims at enhancing the information exchange in all port-related supply chains and between the operators within these supply chains. In recent years, ports have started to create PCS, which refers to an electronic platform including different software modules for logistics actors in the direct port environment as well as in connected subsystems enabling intelligent and secure data exchange between the public and private stakeholders. This complex electronic platform connects multiple systems,

which are operated by a variety of actors within the maritime ecosystem and a plethora of ICT providers. This system can be seen as the "black box" of the maritime sector. (Posti et al. 2012; Polemi 2018.)

The benefits of PCS include that there is no need for bilateral communication or multiple communication methods between operators. With PCS, operators are capable to decrease paperwork, enhance the quality of information, enable data integrity among different port-related operators, and improve delivery times. The ports that have developed PCS are usually large ports and particularly container ports with annual container volume approximately 1 million TEUs or more. There are some Western European ports, such as, ports of Amsterdam and Rotterdam, and port of Hamburg, who have developed a PCS. Still in Finland this is quite a new format for exchanging information between different port operators. In Finland has been developed a national vessel traffic information system, PortNet, which enables the information exchange towards authorities. PortNet cannot be classified as PCS due to its lack of business-to-business interactions. (Posti et al. 2012; Heilig & Voß 2016.)

EU has developed few new technological operations, which should help to ensure the competitiveness and efficiency of European maritime transport sector. For maritime transport sector it is crucial to decrease the administrative burden on ships and to lighten the use of digital environment. First, on 20, October 2010 was developed and started the project of ***National Single Window (NSW)***. The main aim of NSW is to enhance the efficiency, appeal, and environmental sustainability of the maritime sector and advance the integration of the sector to the digital multimodal logistic chain. (European Commission 2015.) Heilig and Voß (2016) have identified the NSW to be "a facility which allows different operators involved in trade and transport to lodge standardized information and documents with a single-entry point to fulfill all import, export, and transit-related regulatory requirements". These NSWs are based on PCS and their security policies need to be evaluated and assessed to guarantee their trustworthy operation (Polemi 2018).

After the launch of the eManifest pilot project was developed the European ***Maritime Single Window (MSW)*** environment, which main aim is to demonstrate the way in which cargo information demanded by maritime and customs authorities, can be delivered together with other reporting forms demanded by Directive 2010/65/EU via a European maritime single window environment. MSW covers the information flows between the data providers of ships, the relevant public authorities, and other Members States via SafeSeaNet (SSN). A data provider of a ship can be either the ship agent, master or the shipping company itself. (EMSA 2017.)

2.6 Developments of the Finnish maritime sector

European ports, more specifically Finnish ports, do not differ greatly from other ports in the world. Finnish ports, as any other in the world, follow industry trends, implement new maritime transport technologies and investigate organizational forms in order to allow them to boost their effectiveness and ease their incorporation in the global logistics chains. (Trujillo & Tovar 2007.) Almost 40% of the freight between the Member States of the EU and over 70% of cargo entering and leaving Europe is transported by sea. Thus, the services of the maritime sector play a key role in terms of the performance of the European economy and quality of life. (Chiappetta & Cuozzo 2017; European Commission 2018.) All of 22 Member States of the EU with a maritime border handle more than 1 200 ports supporting operations of the EU's maritime sector (ENISA 2011). The European ports handle approximately 3,700 million tons of cargo flows, and almost 400 million passengers per year (Chiappetta 2017).

For Finland, the maritime transport represents a critical infrastructure. Over 80% of the foreign trade of Finland is transported by sea. (Yliskylä-Peuralahti et al. 2011.) In the beginning of 2010, Finnish ports handled approximately 5% of the European level volumes (Heijari 2010). The Finnish maritime sector is affected by various actors, which are linked firstly to economy, markets and structure of production, and also the customer needs and service level requirements followed from them (Kallionpää et al. 2013). Finland and its economy and society are highly dependent on the energy, various raw materials, and other supply imports that various industries need. Also, for example, many Finnish export and energy production companies rely on maritime transport as the only transport mode. Ports represents an essential node in the transport network. Additionally, a significant amount of transports is centralized in certain ports. Therefore, any disruptions in the Finnish maritime sector can have negative consequences for supply chains of companies and national security of supply and daily life of people in Finland. (Yliskylä-Peuralahti et al. 2011.)

The Finnish port network has its long history and traditions in terms of the locations of Finnish ports that have been either located near cities or cities have been structured around ports. Until 1995, the cities of Finland had their special rights in terms of maintenance of ports and therefore ports have always been an important part of industrial and commercial activity of municipalities. At the beginning of 2015, all municipal ports were changed to limited liability organizations. There were two ways for this change: a port's assets, among other things, infrastructure and facilities could have been transmitted in the port's balance, or the municipality kept the ownership of the assets and the port and port operators leased or rented the area and facilities. In terms of the cargo handling equipment, the ownership was kept within the port operator, who had owned them previously. The port operators are usually private organisations of which many provide in addition to

stevedoring operations, also services related to the certain port. (Finnish Maritime Society 2011; Karvonen et al. 2016.)

In Finland operates more than 50 ports from which only a few are industry based private ports. This scattered and broad port network of Finland has formed through generations to be more and more market-oriented. In the development of Finnish port network affects economy, market and production structure and as a result of the previous ones the customer needs and service level requirements. (Pöyskö et al. 2014.) Two main maritime clusters are located in Helsinki and Turku. Most shipping companies, the biggest cargo and passenger ports, and one of the largest shipyards (Arctech) are located in Helsinki. The main maritime operator in Turku is the Meyer shipyard. There is also economically important ports and shipping companies located in the Turku region. (Karvonen et al. 2016.)

3 THE CAPTIVATING WORLD OF CYBERSECURITY

3.1 Conceptual illustration of cybersecurity

Figure 5 demonstrates clearly the key concepts of cybersecurity and the relationships of these concepts that are often used interchangeably. In brief, conceptual representation of the role of cybersecurity (C) is as follows. All cyberoperations occur in cyberspace (A), where a system (B) is located. With cybersecurity (C) is protected this system (B). The vulnerabilities (D) of a system with existing cyberthreats (F) and the level of cybersecurity (C) comprise the level of cyberrisk (E) at any given time. If cybersecurity (C) measures are at inadequate level, cyberrisk (E) may materialize through a cyberattack (G), which targets a certain system or systems (B) through an identified or detected vulnerability (D). In practice, a cyberattack (G) can be classified as a materialized cyberthreat (F), which consists of certain specific technical methods to inflict damage. (Ahokas et al. 2017b.)

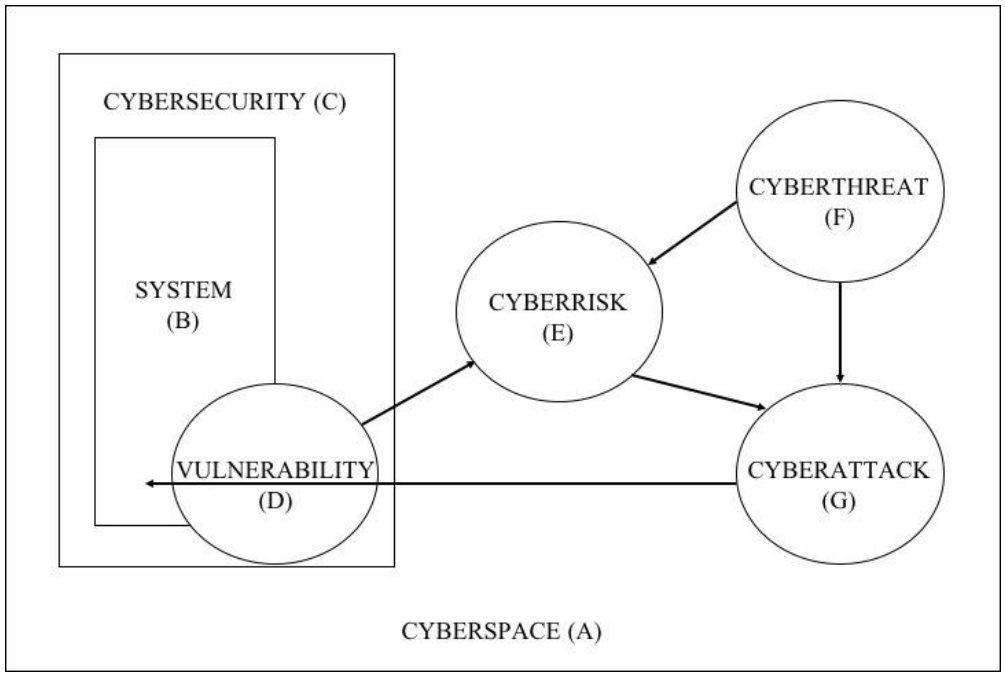

Figure 5 Conceptual demonstration of cybersecurity framework (Ahokas et al. 2017b)

The system (B) refers to all the equipment and software that is closely linked into the cyberspace. The systems can be seen as a part of cybertechnology that refer to the usage of computers or other digital systems in order to store, manipulate, or transmit data, or to handle and monitor physical processes or conditions. An essential aspect of

cybertechnology is that these cybersystems are connected to other systems that provide a possibility for unauthorized persons to intercept, access or change data and the key software. (Tucci 2017.)

3.2 Definition of cybersecurity and related aspects

In order to understand cybersecurity, cyberspace must be identified. Norbert Wiener and Wilson Gibson were the first researchers to take actions towards the identification of cyberspace and its key dimensions. In 1984, Gibson identified cyberspace as "a three-dimensional space where pure information is moved between computer and computer clusters". (Ahokas & Kiiski 2017a.) After the first definitions of cyberspace, many researchers have tried to include technologic dimension into the definitions. These new definitions have included other factors besides technology, such as, computer and computing devices in different networks, in which electronic data is stored and utilized, and communications occurs. (Rantapelkonen & Kantola 2013, 25.)

Cybersecurity is an extremely broad topic (Fok 2013). As a term, it is often used variously and interchangeably with the term information security. It is important to make a clear difference between these two concepts, cybersecurity and information security. The first one goes beyond the boundaries of traditional information security to include also assets, such as humans as users and operators on top of protection of information resources. In cybersecurity, humans are seen as an additional dimension and as potential targets of cyberattacks of even unknowingly participating in a cyberattack. (von Solms & van Niekerk 2013.)

The National Emergency Supply Agency (NESA) of Finland has identified cybersecurity as a state in which threats and risks against the vital operations of societies and/or other operations depending on the cyberenvironment are in control (NESA 2018). In order to have a secure resilience of societies and businesses against cyberattacks, nations and companies need to focus on cybersecurity of critical infrastructures. Cybersecurity is seen as the security of cyberspace in terms of access to, and control and storage of data. (Boyes et al. 2016.) As the objective of cybersecurity, can be seen a stable state, where cyberspace is trustworthy and essential protections are installed (Ministry of Defense of Finland 2013).

Cybersecurity protects all informational assets against a breach or compromise of confidentiality through unauthorized disclosure, integrity through unauthorized modification or destruction, and availability through unauthorized restriction on access (Borum et al. 2015; Muccin 2015; Tucci 2017). Cybersecurity is a vital part in the development of information technologies and by improving it and protecting critical information infrastructures it is possible to protect each nation's security and economic well-being. To

summarize, cybersecurity protects both physical aspects, such as hardware and software, of personal information and technology resources from unauthorized access. (Tonge et al. 2013; Teoh & Mahmood 2017.)

Cyberrisks initiate a complex mix of strategic and operational risks. Strategic risks are concerning the overall direction of an organisation and often appear from its position in the broader business environment. Operational risks contain the performance of an organisation. (Kendrick 2010.) Cyberrisk is an opportunity or vulnerability, which targets to damage the cyberenvironment. When cyberrisk is materialized or it is exploited against an operation depending on the cyberenvironment, it can cause damage, harm or disruption. (Biener et al. 2015; NESA 2018.) In practice, a realized risk may result in financial losses, disruption or damage to the image of an organization from some sort of failure of its information systems (IRM 2014).

Kendrick (2010) has identified two different types of cyberrisks, which are pure risks, and speculative risks. Pure cyberrisks result only in losses. Speculative cyberrisks may contain potential benefits and disadvantages. In terms of cyberrisks, an organisation can structure a cyberrisk team, which objectives include internal audit, risk management, IT security, legal issues, business processes, and procurement.

In the context of cybersecurity vulnerabilities are identified as weaknesses in people, processes and technology (Borum et al. 2015). As a term ***cybervulnerability*** refers to a weakness or a flaw in an asset or system, which is usually a computer or data system, and it is raised either from implementation, design, or other processes that can be exploited or triggered by a threat (Maurushat 2013). A vulnerability can be either direct, such as weak passwords that lead to unauthorized access, or indirect, such as the lack of network segregration (IMO 2016a).

Cybervulnerabilities can be divided into two different categories: 1) potential or unknown vulnerability and 2) confirmed vulnerability. A potential or unknown vulnerability, often referred as zero-day attack, is an undisclosed vulnerability, which has the potentiality to be exploited by a threat. Potential vulnerability can materialize due to hackers, DoS attackers and eavesdroppers. On the other hand, confirmed vulnerability is a vulnerability, which has not been treated and security controls have not been implemented for preventing the exploitation of vulnerabilities. (Kendrick 2010; Polemi 2018.) Maurushat (2013) has classified that a future threat is a vulnerability, which refers to a condition, which may end in harm as a consequence of a previously unknown security vulnerability.

Cyberthreat refers to a threat, which is materialized puts the essential operations of societies and other operations depending on the cyberenvironment in danger (NESA 2018). It can also be understood as the means by which a possible security incident, either intentional or accidental, may occur and affect assets of a certain operator (Polemi 2018). Cyberthreat can be seen as a malicious attempt in cyberspace of which aim is to damage

or disrupt a computer network or system (Boyes et al. 2016). It has been highlighted that the threats against the cyberdomain of organisations is not limited to identity thefts and cybercrime, but also threaten national and international security. Even though, cyber-threats are now well-known, but still the knowledge about their nature is lacking. (Borum et al. 2015.)

From the literature have been indicated five basic cyberthreats, which are hacktivism, cybercriminality, cyberespionage, cyberterrorism, and cyberwar. These main five cyber-threats are presented in Table 1. Each of these cyberthreats has their own individual features relating to actors involved, as well as motivations and objectives behind the actions. (Ahokas & Kiiski 2017.)

Table 1 Characteristics and attackers of cyberthreats

CYBERTHREATS	ATTACKERS	MOTIVATIONS	OBJECTIVES
HACKTIVISM	Hacktivists Hackers Individuals/Insiders	Egoism Political Reputation	Attention Disruptions Knowledge
CYBERCRIMINALITY	Individuals/Insiders Industrial spies Organized crime/Criminals	Economical Informational	Cargo Digital assets Organizational data
CYBERESPIONAGE	Industrial spies Governments Organized crime/Criminals	Ideological Informational Political	Digital assets Knowledge Organizational data
CYBERTERRORISM	Governments Terrorists	Ideological Political Religious Social	Disruptions National institutions Critical infrastructure
CYBERWAR	Governments Terrorists	Egoism Political Religious Social	Military systems National institutions Critical infrastructure

Hacktivism is identified as the operations in cyberspace in which is used various hacking techniques in order to invade into web pages and on computers. With hacktivism can be created pressure on a certain target. (Boyes et al. 2016.) Typical hacking activities may contain compromission of a website, gaining access to and stealing private information, demoralizing data, and the illegal use of credit cards in commercial payment systems (Kendrick 2010).

Cybercriminality refers to all criminal activities in which the primary tools or primary targets are a computer or information systems (Christou 2016; Carrapico & Barrinha 2017). Cybercriminality is mostly used in securing financial rewards through criminal manipulation of Internet technologies. The most typical examples of cybercrime contain the disposition of malicious software, malware, the spreading of virus-infected code or

attacks aiming at threatening the ability of an organisation to operate normally. The last one refers to DoS attacks. (Kendrick 2010.) In 2014, it was calculated that a global cybercrime cost more than USD 400 billion annually, and in 2016 the cost rose to USD 450 billion. These costs include the actual loss, and also recovery and opportunity costs. (Teoh & Mahmood 2017.) Cybercriminality is often divided into four categories: 1) Actions that put the confidentiality, integrity, and availability of data and systems in danger, 2) Forgery and identity thefts, 3) Illegal gambling or spreading false information, and 4) Copyright or brand violations (Luppicini 2014).

Cyberespionage includes illicit access to delicate and private information, such as company strategies, personal information, or intellectual capital. Usually, cyberespionage aims for gaining competitive advantage. (Rittinghouse & Hancock 2003; Boyes et al. 2016.) The losses of cyberespionage include five different types of losses: 1) Loss of intellectual property, business and customer information, 2) Extra costs due to disrupted business plans and competitive exercises, 3) Loss of profits and efficiency, 4) Damage to company reputation, and 5) Increased information technology related security costs (Fitzgerald et al. 2013).

Cyberterrorism and cyberwar are more or less seen to be happening between nations rather than between organisations. Cyberterrorism can be seen as a politically motivated attack towards information, computer systems and software, and databases in the form of a violent invasion by international groups or secret agents (Kapto 2013). As a part of modern information war can be seen cyberwar. In cyberwar, cyberattacks are made against the computer networks of the opponent, which are relevant from the military perspective. (Lewis 2002.) Cyberwar is conducted by using malicious software and viruses to disable military targets (Gross et al. 2017). Cyberwar can be materialized by espionage, website hacking, theft of data, DoS attacks, and infrastructure attacks (Kendrick 2010).

3.3 Cyberattacks and the actors behind them

If cyberrisk is realized, a cyberattack will occur, which has the basic elements of cyberthreats in relation to actors, motives and objectives (Colesniuc 2013). Baltic International Maritime Council (BIMCO) et al. (2017) have divided cyberattacks into two categories: 1) targeted attacks, and 2) untargeted attacks. The difference between targeted and untargeted attacks is that in targeted attacks there is one intended target, which can be an organisation or a system and its data. On the other hand, in untargeted attacks has many different targets. Figure 6 presents the various forms and measures of targeted and untargeted cyberattacks.

Targeted attacks	Untargeted attacks
Brute force	Malware
Denial of Service (DoS)	Social Engineering
Distributed Denial of Service (DDoS)	Phishing
Spear-phishing	Water holing
Subverting the supply chain	Scanning

Figure 6 Forms of targeted and untargeted cyberattacks (BIMCO et al. 2017)

From the targeted and untargeted attacks of Figure 6, the most common attack methods are phishing, malicious software or malware, and DoS attacks (Colesniuc 2013). Phishing refers to emails that are targeted to large amount of people, and usually they include a request to sensitive or confidential data or lure people to visit a fake website. Spear-phishing is targeted version of phishing, it targets a specific person via email, which often include malicious software or links. (BIMCO et al. 2017; Beaumont & Wolthusen 2017.)

Malware is a shorter term of malicious software, which is a piece of software used by a malicious actor to infiltrate, damage, and cause authenticated and unwanted actions on victim's information systems. Malware assess or damages the computer of a victim without the knowledge of the victim, and it spreads by opening infected email attachments or documents. (Fok 2013; BIMCO et al. 2017.) Malware is seen as an efficient and convenient method to execute a cyberattack. Most common types to execute a malware is to use either Trojan, Worms, Exploits, Virus, or Backdoor. In 2015 was globally reported more than 8 million malware attacks. (Teoh & Mahmood 2017.)

DoS floods the network with data to prevent legitimate users from accessing information. A DoS attack can have catastrophic economic results. The shorter DoS attacks, which are measured in hours, effect on the operations of manufacturers that are relying on the right time deliveries. A medium-term DoS attack, which is measured from days to weeks, may result in security issues related to food and fuel. A Distributed Denial of Service (DDoS) has the same method as DoS, but it aims at multiple servers or computers. (Kendrick 2010; Beaumont & Wolthusen 2017; Polemi 2018.)

The uncommon methods of cyberattacks include brute force, subverting the supply chain, social engineering, water holing, and scanning. A cyberattack in which is used brute force as a method, the software or a hacker tries all the possible passwords systematically hoping to eventually find the correct one. Subverting the supply chain includes

compromising software, equipment or supporting services necessary to the targeted organisation. Social engineering is a non-technical technique, which manipulates the personnel of the organisation to brake a cybersecurity procedure, for example, through interaction in social media. In social engineering attacks, the receiver of an email is persuaded to give away his or her user names and passwords. Water holing is a fake website or compromising an authentic website to exploit visitors. Scanning is an attack, which randomly is targeted to a large portion of the Internet. (Fok 2013; BIMCO et al. 2017; Beaumont & Wolthusen 2017.)

There are many different actors behind cyberattacks. ***Cyberattacker*** refers to a person that aims at compromising security in terms of confidentiality, integrity, availability and authenticity, or privacy of an asset. To identify cyberattackers has been formulated attacker profiles, which were presented in Table 1. In Table 1, was also represented the possible motives of the cyberattackers. These attacker profiles are used to identify the relationships of an attacker with the target organisation, such as insider or outsider, his/her skills and goals. Each attacker can be characterized by a triple of attributes, for example, attacker is an insider with premature technical skills, targeting a specific asset or attacker is an outsider with premature technical skills, with no target but to cause general damage. (Polemi 2018.)

Insiders refer to, for example, the employees of a certain company. Therefore, insiders have high-level of access. They work often independently but may give assistance to criminals or hackers. In terms of assistance, insiders may give direct access to criminals into information systems and networks of a certain organisation. The motives of insiders include causing damage or gaining financial benefits. (Beaumont & Wolthusen 2017.)

Hacktivists have high levels of technical abilities in terms of programming skills, which help them to invade to a computer network file and to seek recognition for their technical abilities (Christou 2016). Hacktivist are often related to state-actor or terrorist groups (Beaumont & Wolthusen 2017). There is also with low risk level hacktivist to which are referred as hackers (Kapto 2013).

Hackers are often divided into three categories in terms of their motivations and the level of harm that they cause with their actions. A white-hat hacker aims at promoting general security with his/her actions. A grey-hat hacker has often a criminal background and he/she seeks gaps and vulnerabilities from the systems of various companies. A black-hat hacker is often referred as hacktivist, and they have criminal intentions behind their actions. (Rittinghouse & Hancock 2003; Kapto 2013; Christou 2016.) Hackers are seen as a threat to any network and usually their main objective is to gain access to organisation network through breaching security (Kendrick 2010).

Criminals often aim to gain financial benefits or to inflict personally motivated harm, such as revenge or bullying (Gross et al. 2017). The financial benefit may include criminal damage, robbery of cargo, or identity thefts (European Commission 2013; Boyes et al.

2016). Criminals often take advantage of known vulnerabilities. Criminals have been seen as the current predominant source behind cyberattacks against maritime organisations, especially container terminals. They often aim to extract money in terms of a ransom payment from container terminal operators. (Beaumont & Wolthusen 2017.)

A terrorist is an individual, who has specialized in hacking into computer systems and is capable of organizing individual cyberattacks on global networks (Kapto 2013). Usually, terrorists are seen to inflict damage or incite fear with their actions. Terrorist may aim at causing economic damage, disrupting port operations, or smuggling weapons or other components through ports and the maritime sector with their actions. Terrorists are likely to cause disturbance by using jammers to disrupt wide are Wireless-Fidelity (Wi-Fi) networks or implementing DoS attack against the network of the port operator. (Beaumont & Wolthusen 2017.)

State-actors have high levels of technical ability and are often motivated to gather intelligence and gain military advantages. State-actors usually aim at impacting or disrupting the performance of critical national infrastructures. The earliest reported cyberattack, which was conducted by a state-actor, was the Estonian attack in April 2007, when the country was attacked by a massive wave of botnets. Other state-actor-made cyberattack was made in 2010 and it was called the Stuxnet, which aimed at sabotaging Iranian nuclear enrichment facilities. The Stuxnet was a form of Advanced Persistent Threat (APT), which is a sophisticated and stealth program used to spy or lurk in the computer systems and networks of certain organisation. (Beaumont & Wolthusen 2017; Teoh & Mahmood 2017.)

3.4 Current state of maritime cybersecurity

Over decades, the maritime sector has faced many technological changes and has moved from traditional “paper and fax” culture to adopting modern ICT systems and the use of the internet (Muccin 2015; Kouwenhoven et al. 2016). But not only does the sensitive data of cargo, personnel and vessels in the maritime ICT systems need protection, but also the overall operational control systems can be taken as targets in terms of cyberattacks (Škrlec et al. 2014; Jensen 2017). There have been recognized various types of risk in the maritime ICT systems, from deliberate attacks to unintended, but damaging malwares to simple technical failures. These failures and attacks can compromise the vital safety, security. and environmental functions or may lead to widespread trade disruptions. (Lytle III & Thomas 2015.)

Cyberattacks have taken advantage of the vulnerabilities of MTS, which includes computers, information networks, and telecommunication systems supporting the key port and maritime operations (Hartman & Remick 2015). For example, Somali pirates have

taken advantage of online navigation data, which tracks vessels through AIS, ECDIS and radar, to choose, which vessel to hijack by identifying the cargo loaded on vessels via AIS information (Bosse & Stamer 2017). Hackers have incapacitated a floating oil rig by tilting it and forcing it to shut down, and another malware caused another drilling rig to shut down for 19 days after bringing systems to standstill (Locaria & Wool 2015). The maritime cyberattacks include attacks, such as infiltrating a port's computers, or transmitting fake GPS signals to alter the route of a ship, altering AIS signals of a ship to misreport its location or even accessing ECDIS software to modify maps (Jones 2014; Chiappetta 2017). Because of the dependence on ICT systems, maritime industry is at risk, and has become more vulnerable to disruptions in operations, and is wide open to intentional attacks that may create havoc (Shah 2004).

It can be seen that both ports and vessels have experienced cost-burdening downtime due to cyberattacks. In terms of occurred cyberattacks, maritime operators, such as shipping lines and agents, have lost millions of dollars, because of their email accounts have been compromised and misused. Also, criminals have started to hack the maritime information systems and use them for smuggling purposes. (Jensen 2017.) In terms of ships and its crew, cyberattacks can cause disturbances on critical automation systems which can further cause problems for computer networks (Škrlec et al. 2014). Cyberattacks towards operators of the maritime sector may be extensive, for example, in terms of money and crew safety (Berge 2017). Cyberattacks towards ports' ICSs have the potentiality to bring on disturbance or damage of critical port mechanical devices, such as container cranes, safety and mechanical systems, and even at worst loss of life, cargo pillage, and destruction on ships (Jones 2014; Polemi & Papastergiou 2015).

As indicated in Chapter 3.3, there are various cyberattacks and actors behind them. Nowadays, the worst fear of a maritime operator is to lose the control of the vessel, crew and cargo that can result from cyberattacks conducted by cybercriminals and hackers (Hartman & Remick 2015). There have been drawn horror images on what a cyberattack towards a PCS could result in. Some have estimated that when targeting a PCS with a cyberattack, it could turn LNG tankers within a port into floating bombs. The malfunctioning of PCS may slow down clearance and disturb logistic flows. Only by disrupting or shutting down the ICT systems within a port cyberattackers could endanger emergency responses and cause different types of accidents. (Kouwenhoven et al. 2016; Polemi 2018.) The disruption of MTS and its operations related to global supply chains has the high probability to cause billions of dollars in damage to the economy (Kouwenhoven et al. 2016). It has been evaluated that a disruption of a port can costs between $1B and $2B per a day also effecting Gross Domestic Product (GDP) nationally and regionally (DiRenzo et al. 2015; Jensen 2017).

There has not been many publicly announced cyberattacks in the maritime sector due to reputational damage or because they still have not realized that they have been attacked

(Bosse & Stamer 2017; Jensen 2017). But there has occurred significant cyberattacks within the maritime sector that have woken up the industry's interest. These cyberattacks are represented in Figure 7.

Year of the cyberattack	Name of the virus	Type of the attack	Targeted program or vulnerability	Place of the cyberattack
2018	Unknown	Ransomware	Information technology systems	United States
2018	Unknown	Malware	Communication channels and network	United States
2017	Petya	Ransomware	IT and communication systems	More than 60 countries
2016	Unknown	Phishing	CEO's business email address	United States
2016	Unknown	Hacking	IT and communication systems	Unknown
2016	Unknown	Unknown	Navis, maritime transport logistics software suite	United States
2014	Unknown	Unknown	GPS of port cranes	United States
2013	Icefog	Unknown	Container information system	Japan and Korea
2012	Unknown	Unknown	Cargo systems	Australia
2012	Unknown	Unknown	Lorry-mounted devices and GPS systems	South Korea
2011	Unknown	Unknown	Communication network	Iran
2011	Unknown	Breach	Container information system	Belgium
2010	Unknown	Malware	IT systems	Asia
2001	Aaron	DoS attack	Computers of port of Houston	United States

Figure 7 Publicly reported and known maritime cyberattacks

The most recent cyberattacks towards the maritime sector have occurred in the summer and fall 2018. On September 25, 2018, the port of San Diego suffered a disruption towards its information technology systems, but it has no effect on cargo safety and traffic. Port of San Diego informed that it had received a ransom note from attackers who demanded payment in Bitcoin, but no further comment has been made towards this matter. (Port Technology 2018a.) On July 25, 2018, COSCO shipping company encountered a cyberattack, which effected its communications channels and network applications in their American markets. It has been recognized as malware, which disabled all access to COSCO's Americas website. (Port Technology 2018b.)

But the most significant maritime cyberattack occurred in July 2017, when the container and information systems of Maersk and its port subsidiary APM Terminals were shut down due to the NotPetya cyberattack. This cyberattack took advantage of the computers running Microsoft Windows operating systems, which allowed the attack to spread quickly with relative freedom across multi-national companies. (Tinsley & Sørensen 2017.) This certain cyberattack tells a lot about how the maritime sector is vulnerable in terms of cyberattacks because of Maersk had invested considerable amounts of money in digital safety protocols and was still attacked. The NotPetya cyberattack also highlighted

the increasing sophistication of the different methods which can be used in cyberattacks. (Nadkarni 2017; Kiiski 2018.)

One major cyberattack took place in the port of Antwerp in Belgium between 2011 and 2013, when a drug gang was able to smuggle drugs inside hidden containers, which were misled without early recognition of port operators. The drug gang had hired some hackers to install hidden cameras inside the offices of port of Antwerp and therefore had got access to passwords and the information of containers. (Clark & Keaney 2017; Jensen 2017.) In 2001, occurred one of the first cyberattacks towards ports in United States and it was conducted by a 19-year-old boy named Aaron Caffrey. Caffrey was able to disrupt the computers of the port of Houston, which are used to provide crucial data for shipping pilots, mooring companies and support organisations, who are responsible for assisting vessels to navigate in and out of the port's harbour. (RISI Online Incident Database 2015.)

3.5 Cybersecurity regulations of the international maritime sector

From the interviews was highlighted the importance of the EU's Directive on Security of Network and Information Systems (the NIS Directive), it is important to clarify it in this thesis. The NIS Directive is one of the first EU-wide legislations towards cybersecurity. The aim of the Directive is to provide legal measures to enhance the general level of cybersecurity in each Member State of the EU. The NIS Directive was adopted on 6 July 2016 by the European Parliament and entered into force in August 2016. All the Member States of the EU have to implement the Directive in their national laws by 9 May 2018. In addition to this implementation of the Directive, the Member States are required to identify the key operators of essential services by 9 November 2018. (European Commission 2016.)

In terms of the NIS Directive, all the Member States have been required to set up a Computer Security Incident Response Team (CSIRT), which is the National Cyber Security Center in Finland, and a competent national NIS authority, which is the Finnish Transport Safety Agency. The CSIRT provides current data on cybersecurity situation and helps the key operators and critical infrastructures of each Member State. (European Commission 2016.)

Besides the NIS Directive, there are also few voluntary guidelines published in terms of maritime cybersecurity. These current cybersecurity guidelines for ports and ships start with the identification of threats to different operators. Cybersecurity strategies of ports and ships should include the measures to identify vulnerabilities within port and vessel systems. These cybersecurity strategies should understand and measure the possibility and results of cyberthreats towards all of the systems. (Tinsley & Sørensen 2017.)

The most publicly known voluntary maritime cybersecurity guidelines was presented also in the author's bachelor's thesis (Ahokas 2017). The National Institute of Standards and Technology (NIST) had published in 2014 first guideline for critical infrastructure cybersecurity, and its main target was to identify the five key functions in order to enhance cybersecurity procedures. The five functions were:

- Identify – control of potential risks to systems, resources, and capabilities.
- Protect – implementation of proper safeguards to ensure digital services.
- Detect – measures to identify the cyberthreats and cyberattacks.
- Respond – actions to detect and mitigate against cyberthreats and cyberattacks.
- Recover – actions to support strategies and to restore operations from an attack (NIST 2014).

After the guideline of the NIST in 2016, IMO published its own maritime specific cyberrisk management strategy called "Interim guidelines on maritime cyber risk management" with MSC in Circular MSC.1/Circ.1526 (Tucci 2017). IMO identified that cyberrisk management includes the process of recognition, analyzation, assessing and communicating a cyberrisk. In this cyberrisk management strategy has been included the five functions of the NIST guideline, but they were formed to meet the requirements of the maritime sector. IMO has announced that there is a project running towards making the cyberrisk management on-board ships mandatory as of 1 January 2021, as cited in Resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems as part of the ISM Code, which was implemented in June 2017 after the NotPetya cyberattack. (IMO 2016a, 2016b; Clark & Keaney 2017.)

Some international organisations and institutions have targeted their interest towards cybersecurity and the aspects related to it. For example, the Baltic and International Maritime Council (BIMCO) has published with other key maritime institutions voluntary guidelines and awareness-rising posters that indicate the need to implement cybersecurity into physical security strategies. (Bosse & Stamer 2017; Tinsley & Sørensen 2017.) In 2016, also the Institution of Engineering and Technology (IET) published their Code of Practice for ports and port systems, which includes the Cybersecurity Evaluation and Cybersecurity Plan (Boyes et al. 2016). In 2017, IET published new publication of the Code of Practice Cyber Security for Ships, in which they had taken the perspective of the vessels in terms of cybersecurity procedures (Boyes et al. 2017).

4 RESEARCH METHODS

4.1 Qualitative research and case study

Research strategy refers to all the methodological solutions that were used in the research. From the term of research strategy can be separated a more narrowed concept, research method. The selection of research strategy and single research methods depends on the selected research problem. Most common research strategies can be divided into three traditional strategies: 1) experimental research; 2) survey research; and 3) case study. In an experimental research is measured impacts of one certain variable to another variable. In a survey research, is collected the information in a standardized form from a group of people. In a case study, is collected and analyzed often very detailed and intensive information or data from either a one certain case or a smaller group of cases. Therefore, a case study represents a qualitative research. (Hirsjärvi et al. 2001, 128-131.)

For this thesis, the main research method is a qualitative research, because it can be used to research various disciplines, fields and contents. Qualitative as a term often refers to a stress on processes and meanings that are not precisely analyzed or studied in terms of quality, amount, intensity, and frequency. As a remarkable advantage of qualitative research compared to quantitative research is its ability to understand reality in a social environment, which has been built around various cultural meanings. In qualitative research the case collection and analysis are context bounded, because of the aim of the case collection and analysis is to form a holistic conception from the researched phenomenon. Qualitative research can be conducted by different methods, which involve an interpretative, naturalistic approach to its content. Thus, qualitative researchers examine subjects in their natural environment trying to make sense of or interpret the subject in terms of the meanings of people bring to them. (Denzin & Lincoln 1998; Eriksson & Kovalainen 2008.)

A case study is more efficient research strategy when the research questions relate to understanding of the research phenomenon and especially, when it is crucial to find out, how the phenomenon is seen in practice. (Hirsjärvi & Hurme 2010, 58-60.) Through a case study, the researcher is capable to investigate the phenomenon in historical, economic, social, technological and cultural contexts. A case study also enables the observation of the current phenomena, in which the researcher has no influence on. (Eriksson & Kovalainen 2008.) Either one or multiple phenomena can be investigated in a case study. In business economy, these cases relate to investigation of a specific organisation or a part of the organisation, or they can relate to investigation of a specific operational ensemble, such as, investigation of a process or structural feature of the specific organisation. (Koskinen, Alasuutari & Peltonen 2005, 155-156.)

As earlier mentioned, qualitative approach is used in this research due to the nature of the research object. The purpose of this thesis is to understand and to describe the opinions, attitudes and observations of the interviewees about the research object. The case study was selected as a research strategy because the aim of the thesis is to investigate and observe the research phenomenon in the environment of the key operators of the Finnish maritime trade sector. The case study is used in this thesis also because of it enables to bring out the essential factors of the research object and opinions of the different operators. This research aims at forming a comprehensive conception of the current state of cybersecurity within the Finnish maritime trade sector. The qualitative research is the best method to achieve the aim of the thesis. Qualitative research is also better in terms of the sensitive nature of the phenomenon. One of the aims of the thesis is to gather knowledge and information about cybersecurity awareness among the Finnish maritime trade sector for future best practices and regulations. Qualitative research enables more sincere and open answers from the research object.

4.2 Research object

In a qualitative case study can be used as a source of information both the organisation and the people that are involved in its operations. The possible sources of information of the research material can be divided into six groups:

- documents, such as letter, official reports, and news articles,
- archived data, such as graphs and figures of the phenomenon and statistics,
- interviews,
- direct discoveries,
- participatory observation, and
- physical or cultural artefacts (Yin 2003).

A case study can be usually conducted in practice by using either one or multiple above-mentioned sources of information. However, one of the most significant strengths of a case study is that it enables the usage of several sources of information. With so called triangulation the researcher is capable to form more comprehensive general view of the research phenomenon by using different sources of information to collect the research material. The usage of several sources of information helps the researcher with the justification of the final research results and findings, and with the assertion of the reader about the validity of the results. (Yin 2003.)

At the beginning of this study, the researcher had to outline, which actors of the Finnish maritime sector were included in this study. As a research objects were selected the Finnish maritime trade sector including port authorities, port operators and shipping

companies as the direct actor inside this sector. The researcher of this thesis has not been in any contact with the research objects before this research, which has enabled the subjective observation and interpretation of the research material. As a primary source of research material was used interviews. Besides interviews other important sources of information were news articles considering known maritime cyberattacks and published research articles about maritime cybersecurity. Interviews fulfilled really well the information and data from the published articles due to this fact the validity of collection methods of both research materials could be verified. By means of triangulation of research material were enabled to form more comprehensive general view of the opinions and attitudes of the Finnish maritime trade sector concerning cybersecurity and to notice possible future development proposals.

Researcher set only a few criteria for the selection of interviewees. The decision was made to exclude the ship building companies from this thesis, as the researcher did not see that they are in as direct relationship with the Finnish maritime trade sector as the other three operators: port authority, port operators and shipping companies. For the interviews the most suitable people were selected from each three maritime operator. To have good quality interviews, people with the widest and most exhaustive picture of cybersecurity situation of the company were selected. To gain more comprehensive picture of the Finnish maritime cybersecurity situation, the researcher also decided to interview representatives of the main three Associations of the Finnish maritime sector: Finnish Port Association, Finnish Shipowners' Association, and Finnish Port Operators Association.

4.3 Interviews as collection of the research material

The most significant advantage of interviews compared to other collection methods is that with interviews can be regulated the collection of research material, and the answers and responds can be analyzed in multiple ways. From interview study can be divided multiple different interview methods: 1) structured interview, 2) semi-structured interview, and 3) unstructured or open interview. (Hirsjärvi et al. 2001, 199-204).

One of the targets of this thesis was to formulate a comprehensive picture of the situation of cybersecurity within the Finnish maritime trade sector. Due to this matter, the researcher tried to bring out the opinions and attitudes of the interviewees. The research material was collected to find answers to these beforehand built themes. Therefore, the structured interview would have been too limited and the unstructured interview too open for this kind of research. The semi-structured, or in other words theme interview, was a more suitable interview method for this research due to the purpose and target of this thesis. (Hirsjärvi & Hurme 2010, 47-48.)

The semi-structured interview allows more freedoms for the interviewees. Even though the researcher decides the questions beforehand, the interviewee can answer them in their own words and even suggest new questions. Also, in the semi-structured interview the interviewee can deviate from the original order of the questions. It is essential for semi-structured interviews that they follow the beforehand decided themes instead of more specific questions. The themes or subjects are the same for each interviewee. (Hirsjärvi et al. 2001, 203-204; Hirsjärvi & Hurme 2010, 47-48.)

In each of the interviews almost the same framework was used, the main points were the same, but the interviews were modified to be directed to certain operators. The interview framework is found at the end of this thesis, the Appendix 1. The questions of the interview framework were formed from the themes of this thesis. First, it was crucial to find out the key actors, physical boundaries, responsibilities and the most critical information and communication systems of these actors for each representative. Second, there were questions about cybersecurity and how its factors have been seen by these interviewees and their organisations.

The interview situations were made as natural discussions as possible. Therefore, the beforehand structured interview questions gave support for the interviewer. The interview questions were given also in advance for the interviewees so that they had the time to focus on the responses and really think through the answers. Most of the interviews, that were made face to face, were recorded on the researcher's phone, and during the interviews the key aspects were written down on paper. The recordings were transcripted after the interviews. The names of the interviewees were collected due to recognizing of the interviews, but they won't be brought up in this thesis.

In Table 2, is represented how literature has supported formation of the interview framework. The first background questions considering the operational environment and the basic concepts of cybersecurity has been presented in the following Chapters as presented in Table 2. The last three questions were the ones that needed sights from the interviewees as they represent the Finnish maritime sector in their own expertise fields.

Table 2 Linking the interview framework to the literature Chapters

The purpose of the study	Interview framework	Theoretical inspection
This thesis aims at understanding the effects of cybersecurity factors to the maritime sector, in particular the Finnish maritime sector, and how the different maritime operators and authorities see the responsibilities and obligations concerning cybersecurity and cyberattacks.	**Operational environment**	
	1. How would you define the a) physical borders, b) actors, and c) responsibilities of the organisation you represent?	Chapter 2.4 - The operators of the maritime sector can be divided into: port authorities, port operators, shipping companies, stevedoring, customs
	2. What are the most critical information systems of the organisation you represent?	Chapter 2.5 - The most known critical information systems of the maritime sector are AIS, GPS, ECDIS, PCS, NSW and MSW, and PortNet from the perspective of literature
	Cybersecurity	
	1. How would the organisation define a) cybersecurity, b) cyberthreat, and c) cyberattack?	Chapter 3.2 - Definitions of cybersecurity and related aspects
	2. What kind of cyberthreats or cyberattacks has the organisation encountered?	Chapter 3.3 - Known methods of cyberattacks and actors behind them.
	3. How significant factor cybersecurity is to the organisation you represent?	Chapter 5 - How the representatives of the Finnish maritime sector see, and experience cybersecurity and actors related to it. This kind of information is not found from the recent literature.
	4. What kind of methods the organisation has taken into practice in order to enhance cybersecurity?	
	5. What kind of role has the following actors: a) national authorities, b) cooperation in the industry, c) EU, and d) IMO, in publishing instructions to previously mentioned methods?	

Nine interviews were conducted in total as presented in the Table 3. One of the interviews was only handled by email as the actor had not made significant operations in terms of maritime cybersecurity. One of these interviews was a group interview in which attended three security experts that had knowledge from overall security, land-side security

and ship security. Six interviews were performed in private. Two of these interviews were handled over the phone. One of the interviews was with a cybersecurity expert to conduct and gather more information about the basic ideas and factors of cybersecurity in Finland. Due to the timeline of this thesis and the lack of responses, no port operators were interviewed.

Table 3 Date and durations of the interviews

Interviewee	**Date**	**Duration**
Cybersecurity specialist	20.3.2018	60 min
Port authority	4.4.2018	48 min
Finnish Port Operators Association	2.5.2018	Via email
Finnish Port Association	28.6.2018	1 h 25 min
Finnish Shipowners' Association	6.8.2018	60 min
Shipping company	14.8.2018	12 min
Port authority	6.9.2018	31 min
Shipping company	14.9.2018	40 min
Shipping company	20.9.2018	60 min

In addition to the interviews, the author did also a self-organized research journey onboard a Finnish containership which is operating cargo transports in line service between Finland and seven other countries in the Baltic Sea and in the North Sea Regions. During this trip, the author wrote the literature part of this thesis but also observed the ship-to-port interfaces and the key information systems of the vessel. The information and data from this journey had supported and strengthened the interest of the author towards this issue and world of maritime transport.

4.4 Analysis of research material

One of the hardest and the most difficult steps of the research is to analyze the collected research material. The target of the analyzation is to create clarity and it is used to generate new information about the research subject. The analyzation of the qualitative research begins usually in the interview phase, when the interviewer can make notes from interviewees and categorize them. In other words, analyzation is distillation of meanings, in which the meanings of interviewees are verbalized in shorter form. (Hirsjärvi et al. 2001, 216.)

When the material gathered from the interviews has been recorded, it needs to be transcribed into text. The analyzation of the research material of this thesis was conducted as follows. The material was analyzed and inspected at the same time of the collection of material. Right before the interviews were recorded, they were transcribed into text and saved in the same file. The interview manuscripts were printed out and then the key points were highlighted for efficient usage of the research material.

The classification and organisation of the research material are crucial parts of the analysis. With these aspects are created the basis which enables the later interpretation of the research material. As for the classification of the research material was mainly used the same organisation as in the interview frame. After the classification the research material was connected together in terms of comparison and the formulation of logical general views. (Hirsjärvi et al. 2001, 218; Hirsjärvi & Hurme 2010, 147-149.)

After the classification and organisation of the research material, it should be explained and interpreted. With interpretation is meant that the author debates the results and makes own logical conclusions from them. The target of interpretation is to clarify the research material and the highlighted opinions. It is important to form a logical chain of arguments, because the author, the interviewee and the reader all interpret the research in their own ways because of the factual and facts can create misinterpretations. (Hirsjärvi et al. 2001, 224.) In this thesis was compared the opinions and attitudes of the three Finnish maritime operators about the situation of the maritime cybersecurity. This comparison aimed at bringing out the possible differences and similarities of the different maritime operators.

4.5 Evaluation of the study

The main literature data includes academic articles and research studies published by universities and international institutions, and various maritime articles published by the international maritime sector and the maritime researchers. The greatest improvement compared to the bachelor's thesis of the author (Ahokas 2017) is that she has gathered more valid and accurate articles concerning both issues of this study: the maritime sector and cybersecurity. By gathering data from multiple sources of information, the author has been able to enhance the value of this thesis.

Validity refers to the amount in which a certain claim, result or interpret indicates the object that it is supposed to refer. Validity can be divided into internal validity and external validity. Internal validity refers to the interpretations internal logicality and that there are no conflicts between these interpretations. External validity, on the other hand, refers to the possibility that interpretations can be generalized into other research cases. With valid results and information, the researcher should be able to indicate that his or her

results and observations do not base on false interview statements, questions or interpretations, which have been made in unlikely situation. (Hirsjärvi et al. 2001, 226-227.)

In this thesis, the internal validity was enhanced by the operationalization of the interview themes and questions, and with the interview frame. The internal validity was improved by giving the interview questions beforehand to the interviewees so that they had the time to get to know the themes and key concepts of the interviews. Unfortunately, as the nature of cybersecurity is delicate, the author could not limit the selection of the interviewees any further than by selecting the main operators from the maritime trade sector: port authority, port operators, and shipping companies.

As the interviewees were selected by any other up-front consideration, it can be seen as one of the matters, which has the potential to weaken the reliability of this research. Most of the interviewees worked either in the security or IT departments of the organisations, and this enhances the reliability of the research, because the theme for research is highly connected to security. Before starting the research, the author had no previous contacts with the interviewees or the organisations of the interviewees, and alternatively this matter enhances the reliability of the research but also weakens it. As an external researcher of the organisation it was easier to keep on objective attitude towards the research object, but at the same time the researcher had to explore the research objects more accurately to be capable to form the required context of the researched organisations for the research.

Reliability measures the independence of the research results of the qualitative research from time and the researcher. Thus, in a reliable research the measurement of the cases has been conducted harmoniously. In practice, this refers to by observing, for example, the one and the same person in two various research occasions can draw the same results. Furthermore, two different researchers should be able to draw the same results. (Koskinen et al. 2005, 255; Hirsjärvi et al. 2001, 226-227.) The reliability of this thesis was improved by using an audio recorder during the interviews because of this the transcriptions could be done word for word. Due to the word for word transcriptions the false interpretations were avoided.

The overall reliability of this thesis was enhanced by explaining the research steps and their execution as precisely as possible (Koskinen et al. 2005, 254-255). It is justified to mention that the cases concerned in this thesis are only research example and the results drawn from them should not be solely generalized. Even though, the results can not be generalized to other industries or other maritime operators, they perform as good examples in the understanding the concepts and situation of cybersecurity among Finnish maritime operators.

This research and the cases related to it give meaning to other previous international research, because of this certain thematic entity has been very scantly researched by any scholarly methods. In this thesis, generalization of the research outside the research object

is not as important as the understanding of the whole entity of the research theme, cybersecurity. The saturation did occur in this thesis after the first two interviewees of each actor as the scope of the interviewees was quite broad, therefore the author did not see necessary to fit any more interviewees in this thesis. The reliability of this thesis could have been enhanced by specifying the selection of the interviewees and including all the operators of the Finnish maritime sector.

4.6 Research process

In spring 2017, the author finished her bachelor's thesis (Ahokas 2017), which focused on cybersecurity in ports with the research question: "How cybersecurity effects on ports and other critical infrastructure?". In the bachelor's thesis, the author gathered all the available researches, articles and guidelines that had been published about port cybersecurity. Three main cybersecurity guidelines for ports were founded:

- Cyberrisk Management Strategy for Ports by IMO (2016a),
- Code of Practice by the Institute of Engineering and Technology (Boyes et al. 2016), and
- Framework for Improving Critical Infrastructure Cybersecurity by NIST (2017).

The author worked a year as a research assistant for the HAZARD project, which aims at mitigating the impacts of emergencies in large seaports in the Baltic Sea Region. The emergencies include leakages of hazardous materials, fires on passenger ships at port, oil spills in port areas and explosions of gases or chemicals. (HAZARD project 2018.) In the beginning of the author's career, her bachelor's thesis was further remodeled to a more academic format and published as a part of the HAZARD project's publications by title "Cybersecurity in ports". The research question was formulated to meet more specifically the needs of ports: "What effects does cybersecurity have on ports?". (Ahokas & Kiiski 2017.) This remodeled publication was further enhanced and deepened for the Hamburg International Conference of Logistics in fall 2017. In this new article "Cybersecurity in Ports: a Conceptual Approach" (Ahokas et al. 2017b), the focus on the subject was more conceptual and academic and aimed at simplifying the complexity of cybersecurity in the maritime sector. In this conference article was presented the Figure 6, which authors Ahokas and Kiiski had formulated based on the literature review.

During the career of the author of this thesis, she maintained two Excel-files about the occurred cyberattacks within the international maritime sector, and articles and researches about the maritime cybersecurity. These two files were used as a basis for the Chapters 3.4 and 3.5 in this thesis. The author also participated in port cybersecurity event in summer 2017, which the HAZARD project organized with the Finnish Port Association. The

author also conducted a series of interviews for the key security authority of Finland for their cybersecurity project during the summer 2017. From these interviews, the author got more information and knowledge that the cybersecurity situation in the Finnish maritime sector requires more investigation as the subject has emerged in so many public discussions.

In the beginning of this master's thesis, the author had gathered a great amount of references about the international maritime cybersecurity. The author began the process of this master's thesis by formulating the research question and the structure of the thesis to meet the characteristics of the target group: the Finnish maritime sector. The literature review was deepened with the facts about the differences of maritime safety and security as they are the key factors that control the safety and security procedures of maritime operators around the world. The author organized a self-organized research journey onboard a Finnish containership as earlier mentioned. This trip gave the author more confidence about the importance of the research subject and how important the crew of a containership saw cybersecurity for their operations. During this journey, the author had the chance to explore the safety and security publications of the IMO (2012; 2014a; 2014b; 2016a) and other safety and security certificates by different organisations.

After the journey, the author started to work organize the interviews. First, the author met with the cybersecurity specialist to have more comprehensive understanding about the cybersecurity concepts. While working the summer on a shipping company, the author tried to conduct as many interviews as possible, but most of the interviews was conducted in August 2018. The research material of this master's thesis is based on various articles and researches of international authors, and the interviews which the author of this thesis has conducted.

5 CYBERSECURITY AND THE FINNISH MARITIME SECTOR

5.1 Conceptual map of cybersecurity related aspects

In Chapter 3 was presented Figure 5 the conceptual map of cybersecurity matters, this same Figure was shown to the cybersecurity specialist in the first interview. Motive for this interview was to have structure on how to construct and form correct definitions for different cybersecurity concepts as they occur in literature with broad definitions. From national and organizational perspective, cybersecurity is something, that information security has effect on the physical operations in practice within a nation or in an organisation. Figure 8 is a remodeled version of Figure 5 which has been formed based on the interview with the cybersecurity specialist.

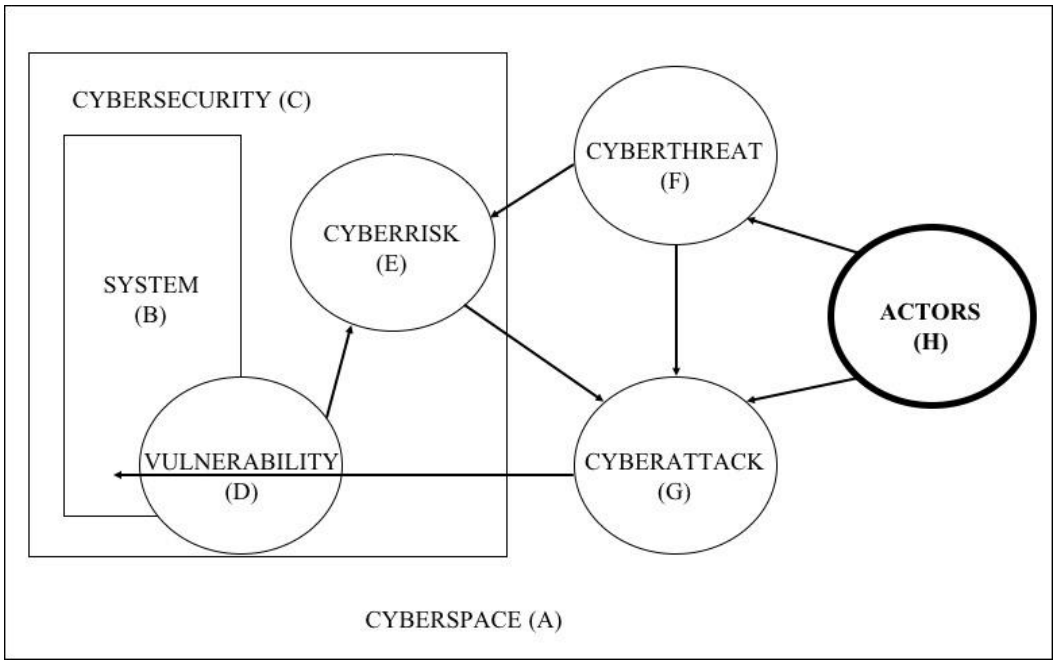

Figure 8 Remodeled framework of cybersecurity related concepts

As system (B) and cybersecurity (C) are represented as parts of an organisation and its operations, cyberrisk (E) because of risk refers to the likelihood of the possibility that something is going to happen. When speaking of cyberattack (G), is often referred only to cyberattack, but it can be possible to divide the successful cyberattacks from the general term. It can also be understood that the word attack requires some sort of actors (H) or attackers who has a motive to do a cyberattack (G) and target at a specific organisation or operator. These actors (H) behind cyberattacks (G) were presented in Chapter 3.3.

5.2 Operational environment of port authorities

According to the interviews, it became clear that the ISPS Code of IMO is the most significant mandatory maritime security Code for ports. ISPS Code regulates the physical borders and areas of ports in Finland and internationally. Ports often do include the surrounding industry factories or other business areas as part of their operational environment. Some of the Finnish ports have their own logistics areas for trailers and containers further away from the main port area. In terms of security and safety, the main physical area in which the port authority is responsible for, is restricted with fences accordingly to ISPS regulations.

Even though the borders are fixed, there are multiple different actors operating inside or near the port area. Usually, inside the fenced ISPS port area are located stevedoring companies or in other words port operators, customs, and other organisation providing service, such as container depot and warehousing operations. As mentioned, there are also other operators near or surrounding the port area, and these are usually industrial enterprises that require the operations of ports and shipping companies in order to move and transport their products and cargo around the world.

The port authority presents itself as the main operator and observer in the port. Port authority is like the host of the port, and through contracts the stevedoring companies and other organisations can locate inside the port area and have all the facilities that they need for their business operations. The security perspective highlights that the port authority and the port operators are together responsible for the port structures. As for the main responsibility for the port authority can be seen that as they own the land areas, they are responsible for all the environmental matters. Port authority also has provided all the necessary infrastructure and facilities for the organisations. From the information technology perspective, the basic infrastructure includes also telecommunications networks and light masts, which the other organisations can rent. But the port operators own their own cranes and other facilities that they require for their own business operations.

As for the critical information technologies, the port authorities saw the general systems and technologies which are needed for the overall operation of the port. The most critical information system is enterprise resource planning (ERP) systems, such as cargo handling systems, in which are handled the information about the location, consignee and destination of different cargo units, such as containers and trailers. Also, one of the main critical systems in a port, is the gate system, which identifies all the units that are entering and leaving the port. It is not as critical as the ERP systems, but if it is out of order, it will remarkably slow down the operation speed of the port and its operators.

5.3 Operational environment of shipping companies

A shipping company can be seen as a business unit, which operates and offers shipping industry operations, which include operating and owning of vessels. It is an actor, who takes care of the maritime transport for its customers by chartering the space onboard a ship. The physical borders of shipping company were harder to identify as the organisation has responsibilities on land in terms of cargo but does not necessarily have any responsibilities about loading of cargo. Shipping companies agreed that the physical borders of a shipping company can be seen as the ship and the voyage. A ship can be seen as an independent unit, but it is under the command of the shipping company. It was also recognized through the interviewees that the electric interfaces between the shipping company and the ships are not as automatized yet, because of their restricted nature.

As actors of a shipping company was seen the ships of the shipping companies that were on time chartering or under other contracts. One shipping company highlighted the importance of the department of information technology as a main actor within the shipping company. The department of information technology is responsible for security matters, such as systems onboard ships.

In general, it is quite clear and simple what is the responsibilities of a shipping company. The area of responsibility, when the shipping company is responsible of the cargo, is the maritime voyage and in other words as long as the cargo is on board of the ship. With the shipping companies operating with own vessels, the responsibility of vessels was clear, it is during the sea voyage. In one of the interviews was highlighted as the responsibility of the shipping company to take care of the technical operations and the safety of the crew.

As critical information systems of the shipping companies rise the operational systems, such as electronic charts, email and cargo programs, ERP systems, and servers. Especially the ERP systems were seen as the most critical information systems in terms of cybersecurity. In terms of ships, the critical information systems include ECDIS and all the safety and security systems that are needed to operate the vessel correctly. One shipping company added as a critical information system the booking systems, which include all the essential information about cargo, even though the disturbance of booking systems only results economical losses, but it does not position any security risks.

5.4 Cybersecurity and the Finnish maritime sector

Before entering the detailed cybersecurity questions, it was crucial to understand how the represented company and the interviewees experienced the key cybersecurity related concepts: cybersecurity, cyberthreat and cyberattack. In general discussion, **cybersecurity**

was more or less associated with information security, but not as a synonym. Port authorities understood cybersecurity as a part of information security, which includes all the equipment and software. It was interesting that so many of the interviewees mentioned the possibility of human error which can lead into cyberattacks. A shipping company connected cybersecurity in a situation in which critical information systems are safe and cyberattacks do not occur. Other shipping company saw cybersecurity as the follow-up of what is happening in the world, recognizing threats, using the best practices and having multiple parallel protections. Only a few of the interviewees could identify cybersecurity as the protection of the entirety, which includes all the software, equipment, personnel and physical facilities. Only one shipping company recognized that cybersecurity had not emerged in security discussions.

Overall, a **cyberthreat** was seen to refer to that there is something on the loose from which is needed to be ready for and protected from. Port authorities saw that cyberthreats as different kind of threats, which include phishing and security breaches. As earlier mentioned, the possibility of human error, it has been now noticed that the biggest threat typically is the organization's own personnel, who do not keep their passwords and user names safe and private. A shipping company saw cyberthreat as anything possible, it can include blackmailing or additional costs and operations even though there are no direct costs from cyberthreats. Other shipping company had learned from the cyberattack towards MAERSK that cyberthreat can be any regular disturbance attacks on physical premises and systems. Cyberthreat can be seen as someone trying to do harm for the entirety, which cybersecurity tries to protect.

Cyberattack was seen as someone trying to either harm or prevent a software or system from operating correctly. Behind a cyberattack can be various motives, such as blackmail or economic benefits from trying to slip a certain cargo unit to the port and onboard ship. Cyberattack materializes when an organisation is targeted or something has happened either for the organisation itself or someone close by. A shipping company saw cyberattack as any intentional attempt to paralyze the main systems and connections. In terms of cyberattacks, the most frightening situation is the one that no one could ever foresee. Cyberattack can be anything that disturbs or paralyzes the operations of an organisation through ransomware or malware or simply by cutting the electric wires.

After having understood the perspective of the representatives' knowledge on the basic cybersecurity issues, it was time to discover **what kind of cyberthreats or cyberattacks** the represented **port authority or shipping company had faced** during recent years. Port authorities had not encountered any maritime sector specific or targeted cyberattacks. Even though, email has been more or less one of the main tools in cyberattacks, and it is often used in sending false payment emails in the name of a chief executive officer (CEO) of a large organisation. These sorts of attacks were not seen as cyberattacks but more as a cyberdisturbance in terms of port authorities.

One shipping company had encountered to identity theft at the organisation level through networks, and onboard of one of its ships had taken a ransomware through USB flash drive. They had also collected statistics that about 50-100 virus emails pass the junk mail filtration daily. Also, on a daily basis, at least 10 pieces of phishing spams, that include offers from port costs, gets through the security methods. Also, one shipping company encounters on a yearly basis various ransomware attacks and encrypted software from external USB flash drives, but none of these attacks has been directed especially towards this shipping company. Even though, one shipping company, which had not recognized the insignificance of cybersecurity, it had encountered email phishing and fake invoices. But these had not risen the attention of cybersecurity and new security methods within the organisation.

It was easier for the interviewees to address **the importance of cybersecurity** for their operations after unveiling the known cyberthreats and cyberattacks of the interviewees' companies. From the perspective of port authorities, cybersecurity is seen as a significant factor as the operations overall in the maritime sector are highly automatized. Some did not see cybersecurity more significant than information security but admitted that as the knowledge and awareness increases will the significance of cybersecurity also increase. It was very well recognized that as the automatization of software and operations increases, so does the awareness and significance of cybersecurity.

A shipping company saw cybersecurity as an essential part of security factors and hoped that there could be more resources in terms of cybersecurity. Other shipping company saw that the cybersecurity matters are significant because they are the main responsibility of the department of information security as they are preventing and developing methods towards cyberthreats and cyberattacks. One of the shipping companies did not see cybersecurity as significant factor as other interviewees, because of it thought that cybersecurity is more important for the shipper as they possess more detailed cargo information, which is more delicate for cyberattacks. The organisation saw that in the future cybersecurity will rise more significant towards ship's navigation and other data systems especially in terms of safety of the crew.

The fourth cybersecurity question focused on the **methods** that the representatives' organisations had taken into action in order t**o enhance cybersecurity**. Port authorities have taken multiple different methods in order to enhance their cybersecurity matters. All have invested money on their technical methods and also improved their personnel education and guidance about cybersecurity. Technical methods include firewalls and junk mail filtrations, and different segments of the network. As with the port authorities highlighted, so did the shipping companies highlight the fact that the education and raising the awareness of personnel as the key method son improving cybersecurity within the organisation. Beside these personnel improvement, one shipping company had also made technical changes in terms of computers and servers keeping them updated on time. Other

shipping company brought up the segmentation of networks as one of the methods of enhancing cybersecurity, this will restrict the attack and it can be more easily targeted with preventative methods.

The fifth cybersecurity question was formed to understand **the role of different national and international authorities** in terms of enhancing cybersecurity procedures. It was clear that the National Cyber Security Center of Finland and NESA have had the most effect on enhancing the awareness and best practices of cybersecurity overall in Finland and within different industries and critical infrastructures. One of the interviewees highlighted that National Cyber Security Center of Finland offers free of charge help and guidance on security of supply critical operators. Other interviewee mentioned that from the NESA and the National Cyber Security Center has come up new industry specific notification channels. Also, the Finnish Communications Regulatory Authority has published information security guidance and snapshot on the current situation of cybersecurity in Finland.

As indicated earlier in this thesis, there are three main Associations for the Finnish maritime sector: the Finnish Port Association, the Finnish Shipowners' Association, and the Finnish Port Operators Association. From the interviews was highlighted that these Associations have focused on informing and putting forward new instructions or publications considering cybersecurity at their fields of operation. They were assured that each organisation and operator of their Association has taken steps towards more secure and safe operations in terms of cybersecurity.

The role of the EU was seen not as significant as it could be. Each interviewee highlighted that the EU takes good care of the digital safety of its critical infrastructures and industries through overall guidelines and legislations, but still industry specific legislations have not been published. All the interviewees saw that the NIS Directive is one of the significant legislations of EU towards cybersecurity. The NIS Directive is presented in Chapter 3.5 with some voluntary guidelines of maritime cybersecurity. For ports and especially for port authorities, the Finnish national security authority has started its new project, which aims at simplifying the key elements of the NIS Directive. This task force is considering all the things that the Directive demands from nationally significant ports. It figures out, what the Directive requires from ports, what kind of models for operations are forming, and if there are any minimum requirement levels for information security. The NIS Directive is yet to be implemented into security procedures of the organisations, so it is far too early to foresee how it is going to shape the security methods in the future, and whether it has any significant changes on these security methods.

Some of the interviewees highlighted the new forms of information systems that EU has started to invest in. These are called the National Single Window and Maritime Single Window, these were presented in Chapter 2.5. As the author was in the research journey onboard a Finnish container ship, she witnessed that the NSW and MSW do not work as

planned like it has been ideally explained in the papers and webpages of EMSA and European Commission. There are quite many problems with these projects and data sharing measures. Both are usually structured in an Excel file, which can contain either one report or have multiple sheets. Often in these Excel files cannot be transported information from the vessels' own Excel sheets or systems. These Excel files are sent back and forth via e-mail, which is not the most reliable source of data exchange. During my research journey onboard a Finnish containership, I got to witness the complexity and slowness of the NSW and MSW Excel files in action.

Even though, IMO is the main maritime organisation in terms of maritime safety and security legislations, it was acknowledged that the legislation procedures take a lot of time to become mandatory and to be implemented into practice. The port authorities have not seen any new publications or instructions published from IMO in terms of cybersecurity. One shipping company was not so hopeful for IMO's instruction about cybersecurity as these instructions usually take a long time to come mandatory or published. One shipping company had noticed that IMO had published cybersecurity guidelines that shipping companies should take into consideration. They also mentioned that in the ISM Code has been highlighted the threats in which every actor in the maritime sector should notice and prevent from.

6 CONCLUSIONS AND IMPLICATIONS

6.1 Main findings of the study

It has been globally noticed that the number of cyberattacks has been growing and the awareness of cybersecurity has increased, but still there is a lot to be done in terms of industry wide best practices and other methods mitigating cyberthreats and cyberattacks. The research question of the study: "How does the Finnish maritime sector experience cybersecurity" aimed at understanding the attitudes and thoughts about cybersecurity and responsibilities related to this matter, and to form a general view of the Finnish maritime sector itself and of the cybersecurity situation. The structure of this study represents the research steps that the author followed during the process.

The study started with understanding the concepts of risk, vulnerability, and threat to further understand how maritime security and safety differ from each other, and how these two concepts have reformed the maritime industry as a whole and the operations of the global and Finnish maritime sector. The critical information systems of the maritime sector were presented in order to highlight the number of different information systems that the maritime operators rely on in terms of securing the maritime transports more. Second, the concepts of cybersecurity and aspects related to it were presented just to clarify the field that this study focused on. Also, in the third Chapter was presented the known maritime cyberattacks and guidelines for maritime cybersecurity. Based on the literature review and the research question, the interview framework was formatted, and the interviews were made in spring and fall 2018. Finally, research material of the interviews was transcripted and analyzed.

As Chapter 2 presented the operators and operations of the global and Finnish maritime sector, the insights of the interviewees supported the idea about the port authority's responsibility. The main responsibility of the port authority is to provide the basic infrastructure to the port and through different contacts with the port operators, shipping companies and other operators can modify the infrastructure and superstructure of the port in order to meet the needs of the operators. Port operators and shipping companies are together responsible for the cargo during their own operations. Port operators handle the cargo, especially the loading and discharging operations of vessels. Shipping companies, on the other hand, may handle the booking of the cargo on board vessels and usually they own the vessels which the port operators load and discharge. Port operators and also shipping companies are responsible of their own information systems and that the operations are undisrupted at all times.

Cybersecurity and the related concepts are quite well understood among the Finnish maritime sector. But as indicated in the Chapter 3, there are various cyberthreats and

cyberattacks that make it difficult to really understand when a company has been attacked and what kind of actors can be behind these cyberattacks. Even though, there are many critical information technologies and systems used by the maritime operators, from the interviews emerged that most of the cyberattacks are directed via emails to different companies. In addition to these email-based cyberattacks, there was few examples about the vulnerability of the ICT systems of vessels in terms of updates of ECDIS, as this was indicated as one of the most vulnerable ICT systems in the literature also. Chapter 3 presented the current situation of the international maritime cybersecurity by introducing the known cyberattacks and different horror pictures of what cyberthreats can place for the maritime operators.

Even though cybersecurity has been noticed amongst the operators of the Finnish maritime sector, it was not quite clear that if cybersecurity should be investigated from the maritime safety or maritime security perspective. Some could see cybersecurity as part of the maritime safety that mitigates unintentional and natural danger, harm, risk and loss, as in some cyberattacks, such as MAERSK was only an outsider victim of the NotPetya cyberattack. But other cyberattacks have been more directed towards a certain maritime operator, which emerged from the interviews. Therefore, cybersecurity should be investigated from the maritime security perspective as it aims at defending the maritime sector against hazard and intentional illicit acts, such as piracy, terrorism, and other criminal activities.

Other interesting result was that how many of the represented maritime operators relied on the outside information security provider as for their information technology security in terms of firewalls and vaccines. It can be said that only the biggest maritime operators were able to really specify cybersecurity as its own security operation instead of being part of information security operations. Also, the biggest maritime operators had been investing time and money in order to educate and enlighten their personnel about the cybersecurity and related factors in terms of better cybersecurity awareness inside the organisation.

In literature has been highlighted the lack of cybersecurity instructions of the critical maritime infrastructure within the most known safety and security regulations: SOLAS, ISM, and ISPS. ISPS Code provides some guidelines on information technology security, but these are at more general level, and lack direct tools, roles and methods for cybersecurity procedures. (Trimble et al. 2017.) Other researches about maritime cybersecurity have highlighted that there is a massive need for comprehensive cybersecurity strategies for the global maritime sector (Kouwenhoven et al. 2016). Also, the interviewees had noticed that there has not been much work done towards better cybersecurity methods by national and international authorities, the EU and IMO. Only one major step has been taken by the EU to enhance cybersecurity among the key operators of the essential services of its Member States, and this has been done by adopting the NIS Directive.

To summarize the results of this thesis and the interviews, there is never too much of knowledge and procedures in terms of cybersecurity procedures. It is a relief to say that overall the situation of cybersecurity is good among the Finnish maritime sector. Each operator has taken either smaller or bigger steps towards better cybersecurity procedures. Earlier, the overall idea from the maritime cybersecurity literature was that the maritime operators do not require or need any mandatory methods to mitigate cyberthreats and cyberattacks (Beaumont & Wolthusen 2017), but this way of thinking has changed, perhaps because of the recent maritime cyberattacks have shown the scale on which cyberattacks can paralyze the operations of any maritime operator. Some of the biggest operators see the mandatory cybersecurity regulations as an important method to increase cybersecurity awareness and mitigation of cyberattacks. But still some of the small operators are waiting mandatory methods before they are willing to significantly enhance their operations in terms of cybersecurity.

It was also clear that quite many operators of the Finnish maritime sector rely on the distance of Finland compared to other countries in the world. If the maritime operator has its operational environment close to Finland, perhaps in the Baltic Sea Region, it did not see itself considerably involved in the international trade. In Finland, the NIS Directive is going to change things significantly for cybersecurity awareness. Even though, not all the maritime operators are directly involved in the task force of Finland, but there is hope and proof that the operators will take a closer look on the results of the task force. The results of this study have the potential to improve the awareness of the importance of cybersecurity for different maritime operators in Finland, and perhaps give some guidelines for the key safety and security authorities of Finland on how to approach the cybersecurity developments from the perspective of the Finnish maritime sector.

6.2 Limitations of the study and proposals for future researches

As for the previous research have focused on the technical matters of cyberthreats instead of the human dimension (Borum et al. 2015), this thesis aimed to understand the human perspective on how cybersecurity effects on the operations of the maritime operators. In the introduction of this thesis was presented to major limitations: the novelty and diverse nature of the topic, and the lack of comprehend terminology behind cybersecurity, which were also challenged during this thesis. Even though, the author had gathered broad information about of the Finnish maritime sector, she did not get the chance to interview any port operators due to timing and external factors.

As for future researches, the author sees that is important to conduct a new survey for a bigger research group. It would also be interesting to evaluate the process of the NIS Directive task force in Finland, and how eventually this legislation falls into its place

inside the Finnish maritime sector. Future research questions could contain some of these suggestions:

- What kind of operations and changes does the NIS Directive require from the Finnish maritime sector?
- How does the Finnish maritime sector experience the requirements of the NIS Directive?

These maritime cybersecurity research require a great number of experts and maritime operators to cooperate in order to establish new information about the specific legislations, guidelines and best practices. The maritime cybersecurity is changing continuously. It has been interesting to see how much within one year between the bachelor's thesis (Ahokas 2017) and this master's thesis of the author the maritime cybersecurity matters have gone further, and the awareness has increased significantly. Within this research subject, maritime cybersecurity, will be more and more factors and actors to be researched and understood at more general level to increase the awareness of cybersecurity even more.

REFERENCES

Ahokas, I. – Laakso, K. (2017) *Delphi study on safety and security in the Baltic Sea Region ports.* Publications of the HAZARD Project. <https://blogit.utu.fi/hazard>, retrieved 17.7.2018.

Ahokas, J. (2017) *Cybersecurity in ports*. Bachelor's thesis. Turku School of Economics, Turku,

Ahokas, J. – Kiiski, T. (2017a) *Cybersecurity in Ports*. Publications of the HAZARD Project. <https://blogit.utu.fi/hazard/what-effects-does-cybersecurity-have-on-ports/>, retrieved 14.8.2018.

Ahokas, J. – Kiiski, T. – Malmsten, J. – Ojala, L. (2017b) Cybersecurity in Ports: a Conceptual Approach. In: W. Kersten, T. Blecker and C. M. Ringle (Eds.). *Digitalisation in Supply Chain Management and Logistics*. Proceedings of the Hamburg International Conference of Logistics (HICL), 23. epubli GmbH, Berlin. 343–359.

Andritsos, F. – Mosconi, M. (2010) Port Security in EU: A Systematic Approach. *2010 International Waterside Security Conference*, WSS 2010, art. no. 5730222.

Attard, F. (2014) IMO's Contribution to International Law Regulating Maritime Security. *Journal of Maritime Law and Commerce*, Vol 45 (4), 479–565.

Baltic and International Maritime Council (BIMCO) – International Chamber of Shipping (ICS) – INTERCARGO – INTERTANKO – Cruise Line International (CLIA) (2017) *The Guidelines on Cyber Security Onboard Ships, Vol 2.0*. BIMCO, Copenhagen.

Beaumont, P. – Wolthusen, S. (2017) Cyber-risks in maritime container ports: An analysis of threats and simulation of impacts. *ISG MSc Information Security thesis series 2017*, Royal Holloway University of London.

Becker-Heins, R. (2014) *ECDIS BASICS – A Guide of the Operational Use of Electronic Chart Display and Information Systems.* 1st Edition. Geomares Publishing, Lemmer. 17–23.

Berge, R. (2017) Maritime cyber security: Good, better & best. *Maritime Reporter and Engineering News*, Vol 79 (5).

Biener, C. – Eling, M. – Wirfs, J. H. (2015) Insurability of Cyber Risks: An Empirical Analysis. *The Geneva Papers on Risk and Insurance – Issues and Practice,* Vol 40 (1), 131–158.

Borum, R. – Felker, J. – Kern, S. – Dennesen, T. F. (2015) Strategic cyber intelligence. *Information & Computer Science*, Vol 23 (3), 317–332.

Bosse, C. – Stamer, M. (2017) Detect and Control Cyber Risks in the Maritime Supply Chain. *Port Technology International (PTI) Journal*, Vol 74, 93–94.

Bou-Harb, E. – Kaisar, E. I. – Austin, M. (2017) On the Impact of Empirical Attack Models Targeting Marine Transportation. *5th IEEE International Conference in Models and Technologies for Intelligent Transportation Systems (MT-ITS),* Napoli, Italy, June 26-28.2017.

Boyes, H. – Isbell, R. – Luck, A. (2017) *Code of Practice - Cyber Security for Ships*. The Institution of Engineering and Technology (IET), Stevenage.

Boyes, H. – Isbell, R. – Luck, A. (2016) *Code of Practice - Cyber Security for Ports and Ports Systems*. The Institution of Engineering and Technology (IET), Stevenage.

Brooks, D. J. (2010) What is security: Definition through knowledge categorization. *Security Journal*, Vol 23 (3), 225–239.

Brooks, M. R. – Cullinane, K. (2007) Governance Models Defined. In: M.R. Brooks and K. Cullinane, ed. 2007. *Devolution, Port Governance and Port Performance*. Elsevier, London. 405–435.

Bueger, C. (2015) What is maritime security? *Marine Policy*, Vol 53, 159–164.

Burton, J. (2016) Cyber Attacks and Maritime Situational Awareness Evidence from Japan and Taiwan. *2016 International Conference on Cyber Situational Awareness, Data analytics and Assessment (CyberSA)*, London, United Kingdom.

Carrapico, H. – Barrinha, A. (2017) The EU as a Coherent Cyber(Security) Actor. *Journal of Common Market Studies*, Vol 55 (6), 1–9.

Chiappetta, A. (2017) Hybrid ports: the role of IoT and Cyber Security in the next decade. *Journal of Sustainable Development of Transport and Logistics*, Vol 2 (2), 47–56.

Chiappetta, A. – Cuozzo, G. (2017) Critical Infrastructure Protection: Beyond the Hybrid Port and Airport Firmware Security: Cybersecurity applications on transport. *5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS),* 206–211.

Christiansen, M. – Fagerholt, K. – Nygreen, B. – Ronen, D. (2013) Ship routing and scheduling in the new millennium. *European Journal of Operational Research*, Vol 228 (3), 467–483.

Christou, G. (2016) *Cybersecurity in the European Union – Resilience and Adaptability in Governance Policy*. Palgrave and Macmillan, Hampshire.

Clark, J. – Keaney, D. (2017) Shutting the Stable Door after the Cyber Horse Has Bolted. *Port Technology International (PTI) Journal*, Vol 76, 18–19.

Colesniuc, D. (2013) Cyberspace and Critical Information Infrastructure. *Informatica Economica*, Vol 17 (4), 123–132.

Craigen, D. – Diakun-Thibault, N. – Purse, R. (2014) Defining Cybersecurity. *Technology Innovation Management Review*, Vol 4 (10), 13–21.

Dellios, K. – Papanikas, D. (2014) Deploying a Maritime Cloud. *IT Professional,* Vol 16 (5), 56–61.

Demirbas, D. – Flint, H. – Bennet, D. (2014) Supply chain interfaces between a port utilizing organisation and port operator. *Supply Chain Management: An International Journal*, Vol 19 (1), 79–97.

Denzin, N.K. – Lincoln, Y.S. (1998) *Volume 1, The Landscape of Qualitative Research: Theories and Issues.* 1st Edition. SAGE Publishing Inc., Thousand Oaks.

DiRenzo, J. – Goward, D.A. – Roberts, F.S. (2015) The Little-known Challenge of Maritime Cyber Security. *6th International Conference on Information, Intelligence, Systems and Applications (IISA),* July 2015.

Dooling, D. (1994) Navigating close to shore. *IEEE SPECTRUM*, December 1994, 24–31.

Du, W. – Zhengxin, M. – Bai, Y. – Shen, C. – Chen, B. – Zhou, Y. (2010) Integrated Wireless Networking Architecture for Maritime Communications. *11th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, London, United Kingdom.

Eriksson, P. – Kovalainen, A. (2008) *Qualitative Methods in Business Research*. 1st edition, Sage Publications, London.

European Commission (2018) *Transport – Transport modes – Maritime*. <https://ec.europa.eu/transport/modes/maritime/internal_market_en>, retrieved 30.1.2018.

European Commission (2016) The Directive on security of network and information systems (NIS Directive). <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>, retrieved 10.10.2018.

European Commission (2015) *National Single Window – Guidelines*. Final version. D.1 – Maritime transport & logistics. 17 April 2015. Brussels, European Commission.

European Commission JOIN(2013) 1 final of 7 February 2013 on *Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace*.

European Maritime Security Agency (2017) *European maritime single window environment*. <http://www.emsa.europa.eu/related-projects/emsw.html>, retrieved 25.2.2018.

European Network and Information Security Agency (2011) *Analysis of cyber security aspects in the maritime sector*. Published November 2011. ENISA, Greece.

Finnish Maritime Society (2011) *Ports*. <http://www.meriliitto.fi/?page_id=181>, retrieved 23.1.2018.

Fitton, O. – Prince, D. – Germond, B. – Lacy, M. (2014) *The Future of Maritime Cyber Security*. Lancaster University, 15 April 2014.

Fitzgerald, M. – Kruschwitz, N. – Bonnet, D. – Welch, M. (2013) Embracing digital technology: a new strategic imperative. *MIT Sloan Management Review*, Vol 55 (2), 1–12.

Fok, E. (2013) An Introduction to Cybersecurity Issues in Modern Transportation Systems. *Institute of Transportation Engineers (ITE) Journal*, Vol 83 (7), 18–21.

Fransas, A. – Nieminen, E. – Salokorpi, M. – Rytkönen, J. (2012) Maritime safety and security: Literature Review. *Publications of Kymenlaakso University of Applied Sciences, Series B Research and Reports*, No 77. Kymenlaakso University of Applied Sciences, Kotka.

Fruth, M. – Teuteberg, F. (2017) Digitization in maritime logistics – What is there and what is missing? *Cogent Business & Management*, Vol 4.

Frøystad, C. – Bernsmed, K. – Meland, P.H. (2017) Protecting Future Maritime Communication. *Proceedings of the 12th International Conference on Availability, Reliability and Security*, Reggio Calabria, Italy, August 29 – September 01, 2017.

Germond, B. (2015) The geopolitical dimension of maritime security. *Marine Policy*, Vol 54, 137–142.

Goldby, M. (2008) Electronic bills of lading and central registries: what is holding back progress? *Information & Communications Technology Law*, Vol 17 (2), 125–149.

Grant, S.T. – Goodyear, J. (1996) ECDIS: Past, Present and Future. *Science Review 1994 and 1995*, Department of Fisheries and Oceans, Dartmouth.

Gross, M. – Canetti, D. – Vashdi, D. (2017) Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity*, Vol 3 (1), 49–58.

Guldbrandsen, C. (2013) Neptune or Poseidon: implementing EU and global maritime safety law in a national agency. *International Review of Administrative Sciences*, Vol 79 (3), 505–522.

Hartman, A. – Remick, P. (2015) Cyber security & the challenge to the maritime networks. *Maritime Reporter and Engineering News*, Vol 77 (8), 28.

HAZARD project (2018) *About the project*. < https://blogit.utu.fi/hazard/hazard/>, retrieved 5.11.2018.

Heijari, J. (2010) Introduction. In: *Efficiency of the ISM Code in Finnish Shipping Companie*s, eds. Juha Heijari – Ulla Tapaninen, 7–9. Publications from the Centre for Maritime Studies University of Turku, A52.

Heilig, L. – Voß, S. (2016) Information systems in seaports: a categorization and overview. *Information Technology and Management,* Vol 18 (3), 179–201.

Helmick, J.S. (2008) Port and maritime security: A research perspective. *Journal of Transport Security*, Vol 1 (1), 15–28.

Hirsjärvi, S. – Remes, P. – Sajavaara, P. (2007) *Tutki ja kirjoita*, 13. ed. Tammi, Helsinki.

Hirsjärvi, S. – Hurme, H. (2010) *Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö*. Gaudeamus Helsinki University Press, Helsinki.

Hult, F. – Sivanesan, G. (2013) Introducing Cyber. *Journal of Business Continuity & Emergency Planning*, Vol 7 (2), 97–102.

International Civil Aviation Organisation (2013) *Safety Management Manual*. Third edition. ICAO, Montreal.

International Maritime Organization (2017) *GMDSS – Global Maritime Distress and Safety System – Manual*. 9th Edition. IMO, London.

International Maritime Organization (2016a) *Interim Guidelines on Maritime Cyber Risk Management*. IMO, London.

International Maritime Organization (2016b) *IMO Multilingual Glossary on Cyberterms*. IMO, London.

International Maritime Organisation (2014a) *SOLAS – Consolidated Edition*. 6th ed. IMO, London.

International Maritime Organization (2014b) *ISM Code – International Safety Management Code with Guidelines for its Implementation*. 4th Edition. IMO, London.

International Maritime Organization (2012) *Guide to Maritime Security and the ISPS Code*. 2012 edition. IMO, London.

Institute of Risk Management (2014) *Cyber Risk: Executive Summary*. IRM, London.

Jensen, L. (2017) The threat hidden in the depths. *Harbours Review – Cyber security and risk management*, No. 4/2017.

Johanson, F. (2016) Remote Operations towards a Digital Revolution in Container Terminals. *Port Technology International (PTI) Journal,* Vol 72, 54–56.

Jones, S. (2014) Addressing cyber security risks. *Port Technology International (PTI) Journal,* Vol 62, 194–195.

Kadivar, M. (2014) Cyber-Attack Attributes. *Technology Innovation Management Review*, Vol 4 (11), 22–27.

Kajitani, Y. – Cruz, A. – Tatano, H. (2013) Economic Impacts Caused by the Failure of Maritime Global Critical Infrastructure – A Case Study of Chemical Facility Explosions in the Straits of Malacca and Singapore. *Journal of Transportation Security*, Vol 6, 289–313.

Kallionpää, E. – Pöllänen, M. – Mäkelä, T. – Liimatainen, H. (2013) *Suomen meriliikenteen skenaariot 2030 – Taustaraportti meriliikenteen strategiatyöhön*. Trafi Publications 3/2013. Finnish Transport Safety Agency Trafi, Helsinki.

Kapto, A.S. (2013) Cyberwarfare: Genesis and Doctrinal Outlines. *Herald of the Russian Academy of Science*, Vol 83 (4), 357–364.

Karvonen, T. – Grönlund, M. – Jokinen, L. – Mäkeläinen, K. – Oinas, P. – Pönni, V. – Ranti, T. – Saarni, J. – Saurama, A. (2016) Suomen meriklusteri kohti 2020-lukua. *MEAE Publications Enterprises 32/2016*. Ministry of Economic Affairs and Employment, Helsinki.

Kendrick, R. (2010) *Cyber Risks for Business Professionals – a Management Guide*. IT Governance Publishing, Cambridgeshire.

Kiiski, T. (2018) Major Maritime Cyber Incidents: A Review. *Port Technology International (PTI) Journal*, Vol 77, 129–130.

Koskinen, I. – Alasuutari, P. – Peltonen T. (2005) Laadulliset menetelmät kauppatieteissä. Vastapaino, Tampere.

Kouwenhoven, N. – Borrett, M. – Wakankar, M. (2016) The Implications and Threats of Cyber Security for Ports. *Port Technology International (PTI) Journal*, Vol 72, 58–60.

Lappalainen, J. – Vepsäläinen, A. – Tapaninen, U. (2010) Analysis of the International Safety Management Code. In: *Efficiency of the ISM Code in Finnish Shipping Companie*s, eds. Juha Heijari – Ulla Tapaninen, 10–16. Publications from the Centre for Maritime Studies University of Turku, A52.

Lewis, J.A. (2002) Assessing the risk of cyber terrorism, cyber war and other cyber threats. *Centre of Strategic & International Studies (CSIS).*

Locaria, D. – Wool, J.R. (2015) Cyberattacks Threaten Critical Infrastructure. *Risk Management*, <http://www.rmmagazine.com/2015/05/01/cyberattacks-threaten-critical-infrastructure/>, retrieved 27.2.2018.

Loh, H. – Thai, V. (2015) Assessing the risk of cyber terrorism, cyber war and other cyber threats. *Centre of Strategic & International Studies (CSIS).* <https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media /csis/pubs/021101_risks_of_cyberterror.pdf>, retrieved 15.2.2018.

Loukas, G. (2015) *Cyber-Physical Attacks: a Growing Invisible Threat*. Elsevier, Oxford.

Luppicini, R. (2014) Illuminating the Dark Side of the Internet with Actor Network Theory: an Integrative Review of Current Cybercrime Research. *Global Media Journal – Canadian Edition*, Vol 7 (1), 35–49.

Manoufali, M. – Alshaer, H. – Kong, P.-Y. – Jimaa, Shibab (2013) Technologies and networks supporting maritime wireless mesh communications. *6th Joint IFIP Wireless and Mobile Networking Conference (WMNC)*, Dubai, United Arab Emirates.

Marlow, P. B. (2010) Maritime Security: an update of key issues. *Maritime Policy & Management*, Vol 37 (7), 667–676.

Maurushat, A. (2013) *Disclosure of Security Vulnerabilities: Legal and Ethical Issues.* Springer, London.

McNicholas, M. (2008) *Maritime Security – An Introduction*. Elsevier, Oxford.

Meersman, H. – Van de Voorde, E. (2010) Port Management, Operation and Competition: a focus on North Europe. In: C. Th. Grammenos, eds. 2002, 2010. *The Handbook of Maritime Economics and Business*. Lloyd's List, London. 891–906.

Ministry of Defense of Finland (2013) *Finland's Cyber Security Strategy*. Government Resolution 24.1.2013. Ministry of Defense, Helsinki.

Muccin, E. (2015) Combatting maritime cyber security threats. *Maritime Reporter and Engineering News,* Vol 77 (6).

Muthiah, K.V. (2009) *Logistics Management and World Seaborne Trade*. Himalaya Publishing house, Mumbai.

Nadkarni, N. (2017) Fighting the faceless criminal. *Port & Harbours*, September/October 2017, 22–23.

National Emergency Supply Agency (2018) Sanasto. <https://www.varmuudenvuoksi.fi/sanasto>, retrieved 20.2.2018.

National Institute of Standards and Technology (2017) *Framework for Improving Critical* Infrastructure *Cybersecurity*. National Institute of Standards and Technology. Version 1.1. Published January 10, 2017.

Notteboom, T. E. – Rodrigue, J.-P. (2005) Port regionalisation: towards a new phase in port development, *Maritime Policy & Management*, Vol 32 (3), 297–313.

Ojala, L. (1990) *Strategic management of port operations: a theoretical review of the concepts of strategic management with some practical applications to main general cargo ports in Finland*. Publications from the Centre for Maritime Studies, University of Turku, A 8.

Page, E. (2017) Maximizing Maritime Safety and Environmental Protection with AIS (Automatic Identification System). *OCEANS Conference*, Anchorage.

Paixão, A. C. – Marlow, P. B. (2003) Fourth generation ports – a question of agility? *International Journal of Physical Distribution & Logistics Management*, Vol 33 (4), 355–376.

Papastergiou, S. – Polemi, N. – Karantjias, A. (2015) CYSM: An Innovative Physical/Cyber Security Management System for Ports. *HAS 2015: Human Aspects of Information Security, Privacy, and Trust*, 219–230.

Polemi, N. (2018) *Port Cybersecurity – Securing Critical Information Infrastructures and Supply Chains*. Elsevier.

Polemi, N. – Papastergiou, S. (2015) Current efforts in Ports and Supply Chains Risk Assessment. *The 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015),* London, United Kingdom, December 14-16, 2015.

Port Technology (2018a) San Diego Suffers Cyber Attack. < https://www.porttechnology.org/news/san_diego_suffers_cyber_attack>, retrieved 10.10.2018.

Port Technology (2018b) COSCO Fights on Against Cyberattack. < https://www.porttechnology.org/news/cosco_fights_on_against_cyberattack>, retrieved 10.10.2018.

Posti, A. – Häkkinen, J. – Brunila, O.-P. – Tapaninen, U. (2012) Port Community Systems and Their Suitability for the Finnish Port Environment. In: *E-Port – Improving efficiency of Finnish port community by intelligent systems.* ed. Antti Posti, Chapter 2, Publications from the Centre for Maritime Studies, University of Turku, Turku.

Prezelj, I. – Ziberna, A. (2013) Consequence-, time- and interdependency-based risk assessment in the field of critical infrastructure. *Risk Management*, Vol 15 (2), 100–131.

Pöyskö, T. – Mäenpää, M. – Iikkanen, P. (2014) Port operations: competitiveness and development requirements. *Publications of the Ministry of Transport and Communications 17/2014.* Ministry of Transport and Communications, Traffic Policy Department, Helsinki.

Rantapelkonen, J. – Kantola, H. (2013) Insights into cyberspace, cyber security, and cyberwar in the Nordic Countries. In: J. Rantapelkonen and M. Salminen, ed. 2013. *The Fog of Cyber Defense.* National Defense University, Helsinki. 24–36.

RISI Online Incident Database (2015) *The Repository of Industrial Security Incidents*. <http://www.risidata.com/Database>, retrieved 25.1.2018.

Rittinghouse, J. – Hancock, W.M. (2003) *Cybersecurity Operations Handbook*. Elsevier Digital Press, London.

Rodrigue, J.-P. – Notteboom, T. – Pallis, A.A. (2011) The financialization of the port and terminal industry: revisiting risk and embeddedness. *Maritime Policy & Management*, Vol 38 (2), 191–213.

Salokorpi, M. – Rytkönen, J. (2010) Comparing Safety Management Practices. In: *Efficiency of the ISM Code in Finnish Shipping Companie*s, eds. Juha Heijari – Ulla Tapaninen, 17–28. Publications from the Centre for Maritime Studies University of Turku, A52.

Shah, S. K. (2004) The Evolving Landscape of Maritime Cybersecurity. *Review of Business, Saint John's University*, Vol 25 (3), 30–36.

Škrlec, Z. – Bicanic, Z. – Tadic, J. (2014) Maritime Cyber Defense. *6th International Maritime Science Conference (IMSC), Book of Proceedings*, April 28–29, 2014, Solin, Croatia.

Stahl, W. M. (2011) The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity. *Georgia Journal of International and Comparative Law*, Vol 40 (1), 247–274.

Stevens, T. (2013) Cyberspace and national security: threats, opportunities, and power in a virtual world. *Contemporary Security Policy*, Vol 34 (1), 254–256.

Teoh, C.S. – Mahmood, A.K. (2017) National Cyber Security Strategies for Digital Economy. *5th International Conference on Research and Innovation in Information Systems (ICRIIS),* Langkawi, Malaysia.

Tinsley, P. – Sørensen, A.F. (2017) Port and Ship Cyber Security After "NotPetya". *Port Technology International (PTI) Journal*, Vol 75, 96–97.

Tonge, A.M. – Kasture, S.S. – Chaudhari, S.R. (2013) Cyber security: challenges for society – literature review. *IOSR Journal of Computer Engineering*, Vol 12 (2), 67–75.

Trimble, D. – Monken, J. – Sand, A. F.L. (2017) A Framework for Cybersecurity Assessments of Critical Port Infrastructure. *International Conference on Cyber Conflict (CyCon U.S.),* Washington D.C, United States of America.

Trujillo, L. – Tovar, B. (2007) The European Port Industry: An Analysis of its Economic Efficiency. *Maritime Economics & Logistics*, Vol 9, 148–171.

Tucci, A. (2017) Cyber Risk Management Preparing for New Operational Risks. *Port Technology International (PTI) Journal*, Vol 74, 90–92.

United Nations Conference on Trade and Development (2017) *Review of Maritime Transport 2017*. UNCTAD, New York.

Whyte, P. (2018) ECDIS – Navigation in 2018. *Port Technology International (PTI) Journal*, Vol 77, 104–105.

Yin, R. (2003) *Case study research: Design and methods*. 3.p. Sage Publications, London.

Yliskylä-Peuralahti, J. – Spies, M. – Kämärä, A. – Tapaninen, U. (2011) *Finnish Critical Industries, Maritime Transport Vulnerabilities and Societal Implications.* Publications from the Centre for Maritime Studies, University of Turku, A 55.

Appendix 1 Interview framework

Interview framework

The aim of this master's thesis is to understand cybersecurity and the criticality of the related factors from the perspective of the Finnish maritime sector. The main target of the thesis is to understand, how the Finnish maritime operators experience the current situation of cybersecurity and the criticality of cyberattacks. By means of these interviews are strived to form a general view of with which data systems the Finnish maritime sector operators use to communicate with each other and what kind of challenges relate to them. The questions have been divided into two categories: 1) Operational environment, and 2) Cybersecurity.

Operational environment:

1. How would you define the port's
   a. physical borders,
   b. actors, and
   c. their responsibilities?

2. What are the most critical data systems of the represented port authority?

Cybersecurity:

1. How does the represented port authority experience following concepts:
   a. cybersecurity,
   b. cyberthreat, and
   c. cyberattack?

2. What kind of cyberthreats or cyberattacks has the represented port authority encountered?

3. How significant factor cybersecurity is for the operation of the represented port authority?

4. What kind of methods has the represented port authority taken in to practice in order to enhance cybersecurity?

5. What kind of role is below mentioned actors' instructions for the implementation of previously mentioned methods?
   a. national authorities
   b. cooperation within the maritime sector
   c. EU
   d. IMO

More information about the master's thesis:
Jenna Ahokas
jeemah@utu.fi, 044 300 4055